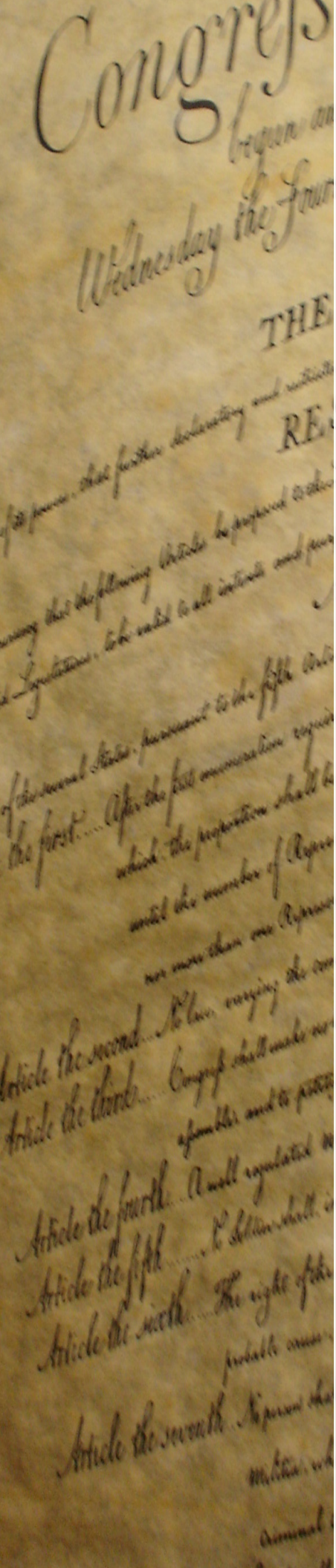

Privacy and Civil Liberties Oversight Board

Second Annual Report to Congress
March 2007 – January 2008

THE WHITE HOUSE
WASHINGTON

THE WHITE HOUSE

WASHINGTON

PRIVACY AND
CIVIL LIBERTIES
OVERSIGHT BOARD

January 30, 2008

Dear Mr. President and Madam Speaker:

The Privacy and Civil Liberties Oversight Board (Board) submitted its first annual report to Congress on April 20, 2007.[1] That report covered activities from the Board's inaugural meeting on March 14, 2006 to March 1, 2007.

On August 3, 2007, President Bush signed into law the *Implementing Recommendations of the 9/11 Commission Act of 2007*.[2] Among other things, this statute reconstitutes the Board as an independent agency within the Executive Branch. All five members will be nominated by the President and confirmed by the Senate for appointment to staggered six-year terms. The chairman will hold a full time position. The statute further provides for a 180-day transition period between the current Board and the reconstituted one.

This report to Congress summarizes the activities of the current Board from March 1, 2007 through the conclusion of its functioning existence on January 30, 2008, and will be the last report from the present Board. It contains no classified information.

I. Background

The *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA)[3] enacted the primary recommendations contained in the *Report of the National Commission on Terrorist Attacks on the United States*[4] (9/11 Commission). Among other matters, the 9/11 Commission recommended the creation of "a board within the Executive Branch to oversee . . . the commitment the government makes to defend our civil liberties."[5] IRTPA responded to this recommendation by creating the Privacy and Civil Liberties Oversight Board.[6]

IRTPA required 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

---

[1] 2007 Report to Congress, *available at* http://www.privacyboard.gov/reports/2007/congress2007.html (last accessed Oct. 1, 2007).

[2] Pub. L. 110-53 (Aug. 3, 2007)

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

[4] THE 9/11 COMMISSION REPORT, 393-94 (2004), *available at* http://www.9-11commission.gov/report/911Report.pdf (last accessed Nov. 1, 2007).

[5] *Id.* at 395.

[6] IRTPA §1061.

policies related to efforts to protect the Nation against terrorism."[7] In carrying out this mandate, the Board had two primary tasks. *First*, it was to "*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"[8] of "laws, regulations, and executive branch policies related to efforts to protect the Nation from terrorism."[9] *Second*, it was to 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."[10] The statute also expressly required the Board to advise[11] and oversee[12] the creation and implementation of the Information Sharing Environment (ISE).

The Board's 2007 Report to Congress summarized the major activities of its first year.[13] Those activities included: (1) organization, administration and process – descriptions of the steps taken to make the Board operational; (2) education and outreach – discussions of how the Board undertook learning about relevant policies and programs and how it reached out to relevant policymakers and interest groups; and (3) issue prioritization – what issues the Board considered and how it evaluated any policies or programs. The 2007 Report also discussed a series of issues and topics the Board intended to address in the upcoming year or years. As a whole, the report presented a Board that had established the necessary infrastructure, internal trust, and external connections to allow it to engage a variety of issues in a substantive and dynamic manner.

The Board personally discussed its first report with the President in a meeting on July 23, 2007. Members believe the initial report may serve as a useful outline of the necessary priorities and activities the reconstituted Board may choose to consider as it works to become operational and effective.

As it did during the first year, the Board's web page, www.privacyboard.gov, continued to summarize the Board's activities. The Board has posted on its web page a number of statements on issues of public interest.

Facilitating the Board's ability to meet its statutory responsibilities was its sound, regular, and productive working relationship with the President's most senior advisors tasked with anti-terrorism responsibilities. These relationships 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.

---

[7] *Id.* § 1061(c)(3).

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

[9] *Id.* § 1061(c)(1)(B).

[10] *Id.* § 1061(c)(2)(A).

[11] *Id.* § 1061(d)(2).

[12] *Id.* § 1061(c)(2)(B).

[13] The Board issued this report in compliance with IRTPA's requirements. *Id.* § 1061(c)(4).

Strong working relationships between the Board and agencies and offices within the Executive Office of the President (EOP) included the National Security Council, Homeland Security Council, Office of Management and Budget, Office of Counsel to the President, and the President's Foreign Intelligence Advisory Board and Intelligence Oversight Board, among others. Additionally, the Board's staff met weekly with an Executive Office of the President working group consisting 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 Counsel to the President, the Office of Legislative Affairs, the Office of Communications, and the Office of Management and Budget.

The Board and its staff were welcomed into all relevant government facilities to observe how agencies operated, developed anti-terror policies, and trained their employees to protect privacy and civil liberties. These visits also promoted a high-quality dialogue between Board Members and advisors.

Because of its position within the EOP, the Board examined issues as part of existing policy development and implementation processes within the EOP and the Executive Branch. The Office of Management and Budget integrated the Board into the Legislative Referral Memorandum process. Through this process, the Board reviewed Administration-wide policies, regulations, and programs that involved its statutory mission.

II. Administrative Activities and Outreach

The Board has met a total of 37 times since the Members were sworn in on March 14, 2006. Formal, full Board meetings averaged twice a month until its final meeting on September 12, 2007. Between the first of March (the end of its first reporting period) and the middle of September 2007, the Board met 13 times. Citing disagreement with the majority of Members over the ability of the Board to meet its statutory responsibilities as a unit of the White House Office within the EOP, Member Lanny J. Davis resigned from the Board on May 14, 2007.[14]

Given the uncertainties created by the introduction and passage of H.R. 1 and S.4 at the beginning of the 110th Congress in January 2007 (discussed further in Section V, below), the Board reluctantly decided to postpone hiring additional staff and obtaining detailees from within the Executive Branch. The Board also decided to postpone any further public meetings until the legislative situation regarding the Board's future was resolved. The Board recognized that the clear Congressional intent to restructure the Board would necessarily implicate its ability to continue to be effective during the interim transition period.

Board staff is taking the steps necessary to close down operations of the present Board. As a unit of the White House Office, its office equipment, supplies, and budget will revert to the EOP. The Board's documents will be transmitted to the National Archives and Records Administration

[14] Former Member Davis' letter of resignation and a discussion of his reasons can be found at http://www.huffingtonpost.com/lanny-davis/why-i-resigned-from-the-p_b_48817.html (last accessed Oct. 3, 2007).

for appropriate preservation and storage.[15] The present Board's staff has consulted with the Office of Counsel to the President and the Department of Justice Office of Legal Counsel on transition issues.

Even as Congress debated the Board's future, the Board continued the outreach and educational efforts begun in the first year. In the past seven months, the full Board, or individual Members at the request of the Chairman, conducted substantive discussions with the following officials:

- The President
    - The White House Chief of Staff
    - The Counsel to the President
- The Attorney General
    - The Assistant Attorney General for National Security
    - The Inspector General of the Department of Justice
    - The Acting Assistant Attorney General for Legal Policy
    - The Chief Privacy and Civil Liberties Officer of the Department of Justice
- The Director of National Intelligence
    - The General Counsel of the Office of the Director of National Intelligence
    - The Civil Liberties Protection Officer for the Office of the Director of National Intelligence
- The Director of the Federal Bureau of Investigation
    - The General Counsel of the Federal Bureau of Investigation
- The Deputy Director of the Central Intelligence Agency
    - The Associate Deputy Director of the Central Intelligence Agency
- The Director of the Terrorist Screening Center
    - The Privacy Officer of the Terrorist Screening Center
- The Deputy Executive Director and Counsel for the President's Foreign Intelligence Advisory Board and Intelligence Oversight Board

[15] Federal Records Act, 44 U.S.C. § 3101.

- The Chief Counsel for the National Counterterrorism Center
- The Assistant Secretary of Homeland Security for Policy
    - The Deputy Assistant Secretary of Homeland Security for Policy

In light of the legislative initiatives designed to restructure the Board, Members and staff met on numerous occasions with Members of Congress and their staff.

- On March 5, 2007, the Chairman, Vice Chairman, and then-Member Lanny Davis met with Senators Joseph Lieberman and Susan Collins.
- On July 24, 2007, the Vice Chairman testified before the House Judiciary Subcommittee on Commercial and Administrative Law.
- Throughout the period covered in this report, the Board's Executive Director remained in regular contact with staff from the Senate Judiciary Committee and Homeland Security and Government Reform Committee, and the House Judiciary Committee, Homeland Security Committee and Intelligence Committee.

On two occasions Board Members met with foreign privacy and civil liberties officials.

- On April 16, 2007, three Board Members met at the State Department with a delegation of Parliamentarians from the European Union to discuss the Board's mission, history, and current activities.
- On October 18, 2007, two Board members met at the British Embassy with a delegation of British Parliamentarians to discuss issues of mutual interest and concern.

III. Policy and Program Review and Analysis

In its 2007 First Report to Congress, the Board identified a series of issues it intended to pursue over the course of the coming year, based significantly on its continued interest in policies and programs reviewed the previous year. The Board also anticipated its Members would be in place through the end of the present Administration. The statutory restructuring of the Board has obviously limited the ability of the Board to meet its original goals. However, a number of substantive policy and program issues were reviewed by the Board in the period covered by this report.

Information Sharing Environment

On September 10, 2007, the Program Manager for the Information Sharing Environment (ISE) in the Office of the Director of National Intelligence (ODNI) issued the *Privacy and Civil Liberties Implementation Guide for the Information Sharing Environment* (Guide).[16] This guide is the

[16] Available at http://www.ise.gov/docs/privacy/PrivacyImpGuide_V1.0_20070912.pdf (last accessed Oct. 2, 2007).

latest step of a process begun in 2005, when the President issued Executive Order 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans*, and a Memorandum to the Heads of Executive Departments and Agencies initiating efforts to establish the ISE, as required by IRTPA. The Memorandum delineated two requirements and five guidelines to prioritize efforts most critical to the development of the ISE and assigned Cabinet officials responsibility for resolving the more complicated issues associated with information sharing.[17] IRTPA requires these guidelines be implemented in consultation with the Board. To facilitate this, the Board's Executive Director was a member of the White House Information Sharing Policy Coordination Committee, which sits above the various working groups and directly below the Deputies and Principals Committees.

The Department of Justice (DOJ) and the ODNI were jointly assigned the lead in developing Guideline 5, concerning privacy and civil liberties rights. Within those agencies, the lead was assigned to the DOJ Chief Privacy and Civil Liberties Officer and the ODNI Civil Liberties Protection Officer, both of whom have worked very closely with the Board since its creation. The Program Manager for the Information Sharing Environment designated them co-chairs of the ISE Privacy Guidelines Committee, which included the Board's Executive Director as a member. This committee consists of the ISE Privacy Officials of the departments and agencies composing the Information Sharing Council. It is intended to ensure consistency and harmonization in the implementation of safeguards for privacy and civil liberties, as well as to serve as a forum for sharing best practices and to resolve inter-agency issues. The ISE Privacy Guidelines Committee will continue to support the ISE and refine its guidance as appropriate.

As discussed in the Board's previous report, the ISE Privacy Guidelines 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. Additionally, the guidelines 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. They are based on core principles that require agencies to: identify an ISE Privacy Official to ensure compliance with the guidelines; 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.

The Guide is intended to assist Federal agencies in implementing the ISE Privacy Guidelines. It provides a framework concentrated on issues at the Federal agency level and describes best practices and a methodology to ensure implementation of the protections and safeguards required by the ISE Privacy Guidelines. As clearly stated, the Guide is not meant to be prescriptive;

[17] 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.

rather the actual process of implementation will be tailored by each agency to fit its unique environment, the data resources it handles, and the specific privacy and civil liberties issues connected to those resources as it implements the guidelines. Each Federal agency is required to develop and implement a written ISE privacy policy setting forth the mechanisms, policies and procedures its employees will following in implementing the ISE Privacy Guidelines, and, to the greatest extent possible, these policies should be available to the public.

It is important to understand that the process of implementing the ISE Privacy Guidelines is an ongoing and evolving process. Agencies will need to evaluate their privacy policy frameworks regularly to take into consideration new issues that arise, new laws passed by Congress, or new guidance issued by the President.

Material Witness Statute

The Material Witness Statute[18] (MWS) allows for the detention of a witness material to a criminal proceeding if the witness' presence cannot be adequately secured by a subpoena or his testimony adequately obtained through deposition. While the authority to detain a material witness can be traced to the First Judiciary Act of 1789, the Bail Reform Act of 1984 most recently amended the text of the present statute.

Under MWS, the government can seek a warrant from a judicial officer in order to arrest a material witness. To do so, the government must file an affidavit with the judicial officer alleging that the individual has information material to a criminal proceeding[19] and it would be impracticable to secure the testimony by subpoena or deposition.

As a direct result of concerns raised by participating representatives of the American Civil Liberties Union and the Liberty Coalition at the Board's December 5, 2006 Georgetown

[18] 18 U.S.C. § 3144 provides:

> *If it appears from an affidavit filed by a party that the testimony of a person is material in a criminal proceeding, and if it is shown that it may become impracticable to secure the presence of the person by subpoena, a judicial officer may order the arrest of the person and treat the person in accordance with the provisions of section 3142 of this title. No material witness may be detained because of inability to comply with any condition of release if the testimony of such witness can adequately be secured by deposition, and if further detention is not necessary to prevent a failure of justice. Release of a material witness may be delayed for a reasonable period of time until the deposition of the witness can be taken pursuant to the Federal Rules of Criminal Procedure.*

[19] While the Supreme Court has never ruled on the issue, since the ruling in *Bacon v. United States*, 449 F.2d 933 (9th Cir. 1971), the phrase "criminal proceeding" includes both trials and grand jury investigations. *See also U.S. v. Awadallah*, 349 F.3d 42 (2d Cir. 2003); *In re Grand Jury Material Witness Det.*, 271 F. Supp. 2d 1266 (D. Or. 2003); *In re Material Witness Warrant*, 213 F. Supp. 2d 287 (S.D.N.Y. 2002). Thus, the MWS authorizes the arrest of those with information material to a grand jury investigation or a trial investigation.

University public forum, the Board decided to review the MWS. It is alleged that this statute was being exploited to detain improperly U.S. Persons suspected of terrorist activity.[20]

The broad concern expressed is that the government may use this statute to detain indefinitely persons suspected of terrorism without charge or probable cause that a crime has been committed. Moreover, due to the secrecy provisions under Rule 6(e) of the Federal Rules of Criminal Procedure, suspects are not always informed of the exact nature of the matter for which they are being detained. The case of Brandon Mayfield of Oregon represents an occasion when the MWS was used to detain an individual in what turned out to be a terrible mistake. Mr. Mayfield was arrested in May of 2004 in connection with the Madrid train bombings of the same year. Mr. Mayfield was detained as a material witness for two weeks without charge before it was later determined that fingerprint identification errors had incorrectly led to his arrest.

At the full Board's request, the Vice Chairman met with officials from DOJ's National Security Division, including the Assistant Attorney General, to investigate the alleged misuse of the MWS.

It is important that adequate oversight and compliance procedures exist to define when the MWS may be used in the anti-terrorism context, minimizing the chance of misuse and holding accountable those responsible for any misuse. The issue before the Board then is whether adequate oversight procedures are in place to ensure privacy rights and civil liberties are addressed when the MWS is used by prosecutors.

Other than the Mayfield case, the Board was not made aware of specific problems with the use of the MWS in the anti-terrorism context. In addition, the Board believes that appropriate oversight exists for three reasons. *First*, Judicial oversight exists at multiple levels. *Second*, the Board was advised that MWS is simply not used by Federal prosecutors in many terrorist-related investigations – indeed, none since the Mayfield case, and the specific approval of the Assistant Attorney General is required for reliance on this legal authority in the anti-terrorism context. *Finally*, Congressional oversight on this matter exists. The policy questions above are being robustly discussed and debated, both in Congress and by the public.[21]

- Judicial Oversight: Whenever the MWS is used by prosecutors in terrorism-related cases, special approval must be obtained by the Assistant Attorney General for the National Security Division. The government then obtains a warrant from a judicial officer. To do so, the government files an affidavit establishing that the individual has (1) information material to a (2) criminal proceeding and (3) it would be impractical to secure the testimony by subpoena or deposition. Once a witness is arrested, the government must demonstrate to a judge within 48 hours that it must continue to hold

[20] The ACLU and Human Rights Watch issued a joint report on this matter in June 2005. In addition, the Liberty Coalition sent a letter to Congress in March 2006 also outlining its concerns with the MWS and endorsing clarifying legislation then pending in Congress.

[21] In addition, the Board believes the common criticism against the government based on the fact that some individuals held as material witnesses under the MWS are never charged with crimes is misplaced. Witnesses are held because of material information they may have related to a criminal proceeding. Use of the statute is not limited to individuals suspected of criminal activity themselves.

that individual for risk of flight. The government must then report to the court on a biweekly basis and identify all witnesses held in custody for more than 10 days.[22] Material witnesses may be represented by counsel.

As Duke University Law School's Civil Liberties OnLine has noted,[23] while detention of a material witness relevant to a grand jury proceeding certainly inconveniences an individual, the detention is subject to judicial review and thus does not necessarily violate civil liberties. Indeed, courts have frequently addressed Constitutional protections in the immigration context and also with respect to non-U.S. Persons.[24]

- Use of MWS Not Common: An overwhelming majority of Material Witness Statute detentions are in matters concerning immigration. It is rare for the law to be used with regard to a matter concerning terrorism. According to the DOJ National Security Division, on only nine occasions since the attacks of September 11, 2001 has the MWS been used in terrorist-related investigations, and, as noted above, it hasn't been used at all since the 2004 Mayfield incident.

- Congressional Oversight of Public Policy Considerations: Congress is aware of the concerns expressed over application of the MWS and has considered proposals to narrow use of the statute. Under discussion are possible provisions that would require the existence of a pending grand jury proceeding or criminal trial before warrants could be issued; impose time limits on the length of detention, thereby ensuring that individuals would not be held for extended periods of time; adopt a heightened showing that the detained witness is an actual flight risk; import due process standards from the Federal Rules of Criminal Procedure to ensure that material witnesses are informed of the basis of their arrest and their right to counsel; require that witnesses be detained in the least restrictive conditions possible (kept separate from those charged with criminal offenses); and require the Justice Department to report annually to Congress on the number of persons held under the material witness laws and average length of detention. [25]

---

[22] 18 U.S.C. § 3144

[23] Available at http://www.law.duke.edu/publiclaw/civil/index.php?action=showtopic&topicid=23 (last accessed Oct. 1, 2007).

[24] *See, Detroit Free Press v. Ashcroft*, 303 F.3d 681 (6th Cir. 2002), (granting public access to immigration hearings based on a First Amendment right); *United States v. Moussaoui*, 382 F.3d 453 (4th Cir. 2004) (court ordered production of material witnesses by the government without allowing any substitutions to such production); *Parlak v. Baker, 3*74 F. Supp. 2d 551 (E.D. Mich. 2005) (affirmed citizen's constitutional right to fair detention pursuant to immigration proceedings when for a reasonable amount of time); *United States v. Koubriti*, 336 F. Supp. 2d 676 (E.D. Mich., 2004) (court condemned the governmental actions denying defendants access to exculpatory evidence during defendants' trial). Most importantly, in *Hamdi v. Rumsfeld*, 542 U.S. 507 (2004), the Supreme Court concluded that a United States citizen, despite being designated an enemy combatant, was entitled to a form of due process, specifically contesting enemy combatant status before a neutral decision maker.

[25] In the 109th Congress, these proposals were contained in legislation introduced by Senator Patrick Leahy, now Chairman of the Senate Judiciary Committee. Available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:s1739is.txt.pdf (last accessed Sep. 28, 2007).

In a meeting with the Board's Vice Chairman, the Assistant Attorney General for the National Security Division stated that he would be willing to discuss the MWS in the anti-terrorism context with interested privacy advocates if they wanted to share their concerns.

Department of Homeland Security National Applications Office

The Department of Homeland Security (DHS) announced in August 2007 its intent to create the National Applications Office (NAO) to facilitate the appropriate use of National Technical Means (NTM), including overhead imagery from satellites, for domestic civil purposes, such as disaster preparation and relief, and homeland security and law enforcement purposes.

NTM has been used for decades to support a variety of domestic users, including scientific, law enforcement and security agencies.[26] Since 1975, most civil requests for this technology went through the Civil Applications Committee at the Department of the Interior. In 2005, the Director of National Intelligence and the Director of the U.S. Geological Survey commissioned an independent study group to determine whether the Intelligence Community was employing NTM capabilities effectively for homeland security and law enforcement purposes. Led by a former director of the National Reconnaissance Office (NRO), in September 2005, this study group determined that many agencies, including those at the state and local level, were unaware of the availability of appropriate NTM capabilities to assist them in achieving their respective missions. It further found that there was an "urgent need for action because opportunities to better protect the nation are being missed."[27] It recommended that the Director of National Intelligence establish a new program to employ NTM for lawful and appropriate civil, homeland security, and law enforcement purposes.

In June 2007, the Director of National Intelligence designated DHS as the executive agent to establish a new program, the NAO. The establishment of this office was the subject of an oversight hearing by the House of Representatives Committee on Homeland Security on September 6, 2007.

The NAO has received initial criticism from Members of Congress and the media. The Board believes that the August 2007 public announcement of this program was not initially well-handled by DHS. Interested Members of Congress have stated they felt they were not properly informed in advance. Incomplete information made available to the public created the impression that the Federal government was undertaking a substantively new program rather than refining, reorganizing, and streamlining existing activities. The Board and the DHS Office

[26] According to the ODNI Civil Liberties Protection Officer, examples of this use include FEMA's use of overhead imagery to examine areas damaged by Hurricanes Katrina and Rita to determine what areas were most in need of assistance. In addition, the U.S. Secret Service uses such imagery to conduct vulnerability studies which depict "line of sight" possibly used by snipers. Law enforcement has used it for high profile events such as the Super Bowl.

[27] Civil Applications Committee Report, September 2005, available at http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB229/27.pdf (last accessed Oct. 3, 2007).

of Civil Rights and Civil Liberties were not brought into the review process as early as they should have been; however, the ODNI Civil Liberties Protection Officer was involved from the beginning.

The Board's staff was eventually briefed on this matter by the DHS Privacy Office and DHS Office of Civil Rights and Civil Liberties, the ODNI Civil Liberties Protection Officer, and staff at the National Geospatial Intelligence Agency. Further, the full Board was briefed at its meeting on September 10, 2007.

The NAO is intended to serve as a central clearing house for requests for access to Intelligence Community capabilities and archived data by civil, homeland security, and law enforcement agencies. These technical collection platforms represent a major investment for the Nation and have been used for a variety of domestic purposes. For example, satellite and other remote sensing platforms have been used for scientific purposes, for border security, and for providing imagery and other data in support of civilian users. The NAO will facilitate access to these and other intelligence capabilities available to the Intelligence Community that have been used in the domestic field. The NAO also is intended to facilitate access to archived data, and to promote the use of unique analytic methodologies and technologies in solving civil, homeland security, and law enforcement problems. The NAO is not authorized to accept requests for the interception or acquisition of communications.

The intent of the NAO is to allow for a more efficient processing and prioritization of requests. Creation of NAO does not, in and of itself, expand the categories of users for whom access to Intelligence Community capabilities is available. Concern has been expressed, however, that its mere existence and the normal incentives to "market" their product will increase the volume of requests, including potentially illegal or inappropriate requests.

DHS states that NAO will work with "customers" to articulate and narrow requests for information, determine whether Intelligence Community capabilities would be able to provide appropriate, useful information, and determine whether commercially available capabilities may satisfy a customer's need. It will also ensure that all requests conform to existing laws and guidance with regard to privacy and civil liberties, including Executive Order 12333 and the Attorney General's U.S. Persons Guidelines. Inappropriate or illegal requests will be denied. In making these determinations, NAO will be advised and supported by three working groups based on anticipated categories of customers: (1) civil applications; (2) homeland security; and (3) law enforcement. The DHS Chief Intelligence Officer has testified that the law enforcement working group is not expected to be operational for at least a year, pending an interagency examination of unique aspects of law enforcement requirements in light of privacy and civil liberties concerns.[28] All three of these working groups will include representatives from the DHS Privacy Office and the DHS Office of Civil Rights and Civil Liberties.

Under the NAO, requests for the use of Intelligence Community capabilities must be accompanied by a detailed written explanation of the purpose and use of the capability. Requests

[28] Testimony of Charles E. Allen before the House Committee on Homeland Security (Sep. 6, 2007).

that raise particularly difficult legal issues will be referred to the NAO's Legal Advisor, and to the DHS Office of General Counsel, if necessary. The NAO also will coordinate any requests that implicate significant or novel legal questions with DOJ, ODNI, and other relevant parties. Approved requests will then be forwarded to the collecting agency. The collecting agency will apply the existing legal standards to ensure: (1) the use is consistent with relevant laws, policies, and regulations; (2) the use of Intelligence Community capabilities does not target collection of information about U.S. Persons in contravention of E.O. 12333 and the Intelligence Community's U.S. Persons rules; (3) the technologies involved in the uses that have been approved are reviewed to determine whether they may constitute a "search" under the Supreme Court's interpretation of the Fourth Amendment to the Constitution;[29]and (4) the forms of approved assistance do not directly involve the U.S. military in law enforcement activities in violation of the Posse Comitatus Act.[30]

Consequently, each request will go through at least three levels of vetting for privacy and civil liberties protection. The first level is with the legal offices at the requesting agencies. The NAO will then review the request and consult with the DHS privacy and civil liberties officials and General Counsel. As appropriate, the NAO will consult with DOJ and other relevant agencies. Finally, the Intelligence Community receiving the request will apply applicable legal standards to all requests. Members of the Intelligence Community can also call upon the expertise of the privacy and legal staff of the ODNI as necessary.

It should be noted, that while technically exempt from most E-Government Act requirements as a national security system, the DHS Privacy Office has nonetheless completed a Privacy Impact Assessment on NAO, which was issued June 15, 2007.[31]

DHS announced on October 1, 2007 that it will postpone creation of NAO to address concerns raised by certain Members of Congress. Based on the information it has reviewed, the Board concludes that this program has now been fully reviewed by numerous offices, that adequate privacy and civil liberties protections will be in place, at multiple levels and in multiple agencies, and that this program should be allowed to commence. The Board further believes this program is consistent with and promotes the spirit of an information sharing environment, as envisioned by IRTPA.[32]

---

[29] Such review will include, among other things, an analysis of the technology at issue under the Supreme Court's decision in *Kyllo v. United States*, 533 U.S. 27 (2001) (holding that use of a thermal imaging device was a search where device was not in general use and revealed interior details of home). The NAO will only process any request that would constitute a search on the condition that a warrant or appropriate court order be obtained, or that a valid, exception to the warrant requirement applies.

[30] 18 U.S.C. § 1835

[31] The PIA is for official use only, and not available to the public.

[32] IRTPA §1016(b)(1)(A)("Information Sharing Environment. – "The President shall create an information sharing environment for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties[.]").

Foreign Intelligence Surveillance Act Modernization

The Protect America Act (PAA)[33] was enacted into law on August 5, 2007 at the Administration's urging, led primarily by the Director of National Intelligence and the Assistant Attorney General for the National Security Division. The Board was asked to review implementation of PAA by the Counsel to the President.

The Foreign Intelligence Surveillance Act (FISA) requires the government to obtain court orders from a specially designated court (the Foreign Intelligence Surveillance Court, or FISC) to conduct certain surveillance or intelligence collection activities. Generally, if an activity falls within FISA's definition of *electronic surveillance*, then the statute requires the government to obtain an order from the FISC authorizing the surveillance. The state of technology in 1978 and the events that preceded the statute's passage suggest that the definition of "electronic surveillance" was crafted with two primary aims: (1) to regulate the government's surveillance of the communications of persons in the United States; and (2) to avoid interfering with certain international signals intelligence activities and other surveillance activities conducted outside the United States.[34]

Given the technology in use at the time of its passage, FISA was designed primarily to protect the privacy of persons in the United States. In the late 1970s, most domestic telephone communications were transmitted by wire. By contrast, most international communications—communications to or from a person in the United States with another person outside the United States—were carried through radio (including by satellite). FISA excluded from the requirement to obtain an order from the FISC the acquisition of most international and all foreign-to-foreign communications. Interestingly, FISA does not require a warrant for radio communications between a person inside the United States and a person outside the United States, unless the government is targeting a particular U.S. person in the United States. Otherwise, only purely domestic radio transmissions require a FISC order. *Additionally*, the events that took place preceding FISA's passage suggest that Congress intended the statute to regulate surveillance of the communications of U.S. Persons in the United States. Specifically, FISA came into being shortly after the conclusion of a series of Congressional hearings that uncovered and highlighted numerous instances of improper domestic surveillance conducted by the Intelligence Community, as well as the improper targeting of the U.S. end of international communications.

Despite the primary intention for FISA to regulate the government's surveillance of the domestic communications of U.S. Persons in the United States, new technologies and communications practices have caused more international communications and some foreign communications to fall within FISA's definition of "electronic surveillance," even where the foreign end is targeted. For example, the use of wire and radio communications has largely reversed itself: most international communications now occur through wire (trans-oceanic cable), and most domestic communications, formerly via wire, now take place by radio. As a result, under the original

[33] Pub. L. No. 110-55 (Aug. 5, 2007).

[34] This point was noted in the legislative history. As the Senate Judiciary Committee report on FISA explained, "the legislation does not deal with international signals intelligence activities as currently engaged in by the National Security Agency and electronic surveillance conducted outside the United States." S. Rep. No. 95-604, at 64 (1978), reprinted in 1978 USCCAN 3904, 3965.

FISA definitions, the government must now generally obtain FISC orders for international wire communications where at least one party to the communication may be in the United States and the communication is acquired in the United States. As noted previously, such international communications generally did not require the authorization of the FISC when they took place via radio (the prevalent practice at the time of FISA's passage). Additionally, current methods of transmitting communications have caused certain purely foreign communications to fall within FISA's definition of "electronic surveillance." The Director of National Intelligence has stated that the resources and time required to obtain FISC orders to acquire these international and foreign communications placed a substantial burden on the Intelligence Community, creating an "intelligence gap."[35]

In an effort to address these changes in technology and communications practices, the PAA excludes from FISA's definition of "electronic surveillance" any "surveillance directed at a person reasonably believed to be located outside of the United States."[36] This amendment does not reference any particular technology but instead focuses on the target of intelligence collection activities. Additional elements of the PAA include:

- The Director of National Intelligence and Attorney General may authorize the collection of foreign intelligence information concerning individuals reasonably believed to be located outside of the United States for periods of up to one year. They may make this authorization only if they certify that five conditions are met:[37]
    - "there are reasonable procedures in place for determining that the acquisition of foreign intelligence information under this section concerns persons reasonably believed to be located outside the United States, and such procedures will be subject to review of the [FISC];"
    - "the acquisition does not constitute electronic surveillance;"
    - "the acquisition involves obtaining the foreign intelligence information from or with the assistance of a communications service provider . . . ;"
    - "a significant purpose of the acquisition is to obtain foreign intelligence information;" and
    - "the minimization procedures to be used with respect to such acquisition activity meet the definition of minimization procedures under section 101(h)" of FISA.
- Within 120 days of enactment of the legislation, the AG must submit to the FISC the procedures to ensure that "procedures by which the Government determines that acquisitions conducted pursuant to [the authorization noted previously] do not constitute

[35] J. Michael McConnell, "Statement for the Record: House Judiciary Committee Hearing on the Foreign Surveillance Act and Protect America Act," (Sep. 18, 2007), available at http://www.dni.gov/testimonies/20070918_testimony.pdf (last accessed Dec. 18, 2007).

[36] PAA § 2.

[37] *Id*. (adding Section 105B to FISA).

electronic surveillance."[38] The Court must approve or reject those procedures. In conducting such a review, the Court may reject the procedures only if it determines that the Director of National Intelligence and the Attorney General have made a "clearly erroneous" determination that the government's procedures "are reasonably designed to ensure that acquisitions conducted pursuant to [the authorization noted previously] do not constitute electronic surveillance." Obviously, this is a fairly deferential standard.

- Third parties (communications service providers, for example) must comply with a lawful directive issued by the Director of National Intelligence and the Attorney General to provide information, facilities, and assistance necessary for the government to accomplish acquisition activities.[39] The government must compensate those third parties for such assistance at the prevailing rate.[40] The recipients of such a directive may challenge its legality before the FISC, the Foreign Intelligence Surveillance Court of Review, and, potentially, the Supreme Court.[41] All such challenges must occur under seal.

- Third parties are given complete civil immunity for complying with a directive issued pursuant to section 105B(e) of FISA.

- These amendments will sunset six months after their enactment.[42] Any authorizations for intelligence acquisition made pursuant to these amendments, however, will remain in effect until their expiration.[43]

- The Attorney General and the Director of National Intelligence shall "assess compliance" with the procedures for determining an individual's location and with the certifications issued pursuant to Section 105B.[44] Both offices must also report instances of noncompliance (both on the part of telecommunications and third parties who are directed to provide assistance for an acquisition and on the part of government actors who fail to comply with the guidelines or procedures established for determining that an acquisition concerns persons reasonably believed to be outside the United States) to the intelligence and the judiciary committees of the House and the Senate on a semiannual basis.[45]

---

[38] *Id*. (adding Section 105C).

[39] *Id*. (adding Section 105B(e)).

[40] *Id*. (adding Section 105B(f)).

[41] *Id*. (adding Section 105B(h)-(k)).

[42] *Id*. § 6(c).

[43] *Id*. § 6(b).

[44] *Id*. § 2 (adding Section 105B(d)).

[45] *Id*. § 4. The Board has not made any recommendations, decisions or assessments with regard to compliance by telecommunications carriers or any other private parties, and has expressed no view on the issue of immunity under the PAA, any other statute, or in connection with any litigation.

In conducting its review, the Board and its staff met with senior individuals within the DOJ and ODNI. The Board met with the Assistant Attorney General for the National Security Division and the Acting Assistant Attorney General for the Office of Legal Policy. Board staff hosted meetings with staff from the Office of Counsel to the President, ODNI, and the DOJ National Security Division. In each meeting, the Board and its staff were able to ask whatever questions they desired and received satisfactory answers to those questions.

In addition to these meetings, Board staff reviewed applicable Attorney General Guidelines and Congressional testimony, and attended Congressional hearings on FISA modernization, with testimony provided by the Director of National Intelligence, Assistant Attorney General for the National Security Division, and various privacy advocates. The Board also received and reviewed a copy of the September 17 letter from the ODNI's Civil Liberties Protection Officer to the Chairman and Ranking Member of the House Permanent Select Committee on Intelligence. Additionally, Board staff has worked closely with the Privacy and Civil Liberties Offices at DOJ and ODNI on matters associated with FISA modernization generally and PAA specifically so that issues of mutual interest and concern were addressed.

In reviewing these documents and meeting with these senior officials, the Board carefully considered five primary issues: (1) The extent to which the PAA allows the government to obtain the communications of U.S. Persons without a court order; (2) whether analysts may intentionally use the PAA to obtain information on U.S. Persons without a FISA Court order where one would otherwise be required; (3) the minimization procedures the government will employ pursuant to the PAA and how those differ from minimization procedures associated with the original FISA legislation; (4) the adequacy of procedures used to determine that acquisition of foreign intelligence information "concerns persons reasonably believed to be located outside the United States"; and (5) auditing, oversight, and other methods that the government will employ to ensure compliance with legal requirements and to limit any bad-faith behavior on the part of individual analysts.

A. To what extent will the PAA allow the government to obtain communications of U.S. Persons without a warrant?

Nothing in the PAA alters the traditional FISA framework requiring the government generally to obtain a FISA court order before it may surveil purely domestic communications or international communications where the target is the U.S. end of that communication. However, the amendments contained in the PAA do allow the government to bypass the FISC court-order process when it targets a person reasonably believed to be outside of the United States. This exception to the FISC-order requirement creates at least two ways in which the government may obtain more information associated with U.S. Persons.

First, as a result of an acquisition concerning a non-U.S. person reasonably believed to be outside the United States, the government might also incidentally acquire information from those (including U.S. Persons) who communicate with the targeted individual. Director McConnell has indicated that the language of the PAA comports with intelligence collection practices—analysts target persons and acquire (subject to minimization procedures) all communications to and from those persons. They cannot, as a practical matter, examine—or even know—all of the persons with whom a target might communicate before beginning collection.

Second, the PAA authorizes acquisition of the communications of a person *reasonably believed* to be located outside of the United States, including a U.S. person. In a situation involving a U.S. person outside the United States, however, the Executive Branch follows the requirements of section 2.5 of Executive Order No. 12333. Under section 2.5, where a warrant would be required for law-enforcement purposes, the Attorney General may authorize the use of a collection technique directed at a U.S. person outside the United States if the Attorney General determines that there is probable cause to believe that the target of the technique is a foreign power or an agent of a foreign power. This determination is very similar to the finding that the FISC must make under FISA, and an application to the Attorney General for a section 2.5 authorization goes through an Executive Branch review process similar to that used in the FISA process.

In either situation, FISA, including the PAA, limits how the government may use information acquired concerning U.S. Persons. The PAA requires the government to employ minimization procedures satisfying the requirements of title I of FISA.[46] In the event information associated with a U.S. person located inside the United States leads the government to want to target that person, the Director of National Intelligence and the Attorney General have assured us that the government will apply to the FISC for a court order authorizing surveillance. FISA, as amended by the PAA, continues to require this.

The ability of the government to obtain the communications of U.S. Persons (incidentally by targeting non-U.S. Persons or by reasonable mistake) leads to two questions: (1) are there adequate minimization procedures in place; and (2) what kind of tracking or auditing program exists to determine if analysts have complied with the applicable minimization procedures (both discussed below)?

B. May analysts intentionally use the PAA to obtain information on U.S. Persons without a FISA Court order?

This question refers to *reverse targeting* whereby an analyst might superficially target a person outside the United States, but for the actual purpose of acquiring information concerning the "real target"—a person (including a U.S. person) inside the United States—without obtaining a FISA court order. The Director of National Intelligence and his staff reject this suggestion based primarily on efficiency and the necessity of obtaining a regular FISA order in such situations. If the government wishes to obtain the communications of a person inside the United States, it is extraordinarily inefficient to attempt to target a series of persons outside the United States; rather, the government would need to obtain all of the communications of the person inside the United States; and to do so would require obtaining an order from the FISC.

The Board believes that, as a result of several factors, reverse targeting is unlikely to occur with any frequency, if indeed it occurs at all. First and most importantly, designating a nominal foreign target where the real target of intelligence interest is a U.S. person inside the United States is prohibited by FISA and the PAA. FISA is a criminal statute, and any official who intentionally goes about trying to circumvent its requirement of obtaining a court order to target

[46] *Id*. § 2 (adding Section 105B(a)(5)).

the communications of a person inside the United States is risking criminal prosecution.[47] Second, the inefficiency of reverse targeting provides a natural incentive against engaging in the practice. If an intelligence agency suspects a U.S. person is an international terrorist or foreign agent, it has a strong incentive to obtain a FISA court order, as noted above.[48] Finally, agencies within the Intelligence Community have auditing procedures to uncover any rogue actors engaging is such activity, and engage in regular training for any personnel involved in signals intelligence operations. Auditing regimes are strict, and the training strongly emphasizes the need to protect the privacy rights of U.S. Persons.

C. How adequate are the minimization procedures required by the PAA and the original FISA legislation?

PAA minimization procedures are those required by FISA and are defined in 50 U.S.C. § 1801(h). No controversy has surfaced regarding the adequacy of those procedures. The Board was briefed on the classified minimization procedures in place.

D. How adequate are the procedures used to determine that the acquisition of foreign intelligence information "concerns persons reasonably believed to be located outside the United States"?

This question corresponds with the general concern that the government will have the ability to acquire more easily the communications of U.S. Persons without a FISA court order. Critics point to two ways in which the PAA and these procedures could allow for increased surveillance of persons in the United States without court approval. *First*, although the FISC must approve the procedures used to determine that an acquisition does not constitute electronic surveillance, the court must defer rather strongly to the government's construction of the procedures. The FISC may reject the procedures only if it determines that the "Government's determination . . . that those procedures are reasonably designed to ensure that acquisitions conducted pursuant to section 105B do not constitute electronic surveillance" is "clearly erroneous."[49] *Second*, some critics have asserted that the use of the word "concerns" suggests that surveillance may go beyond merely targeting persons reasonably believed to be outside the United States. Under this argument, information might "concern" both a person outside of the United States and a person inside the United States, which could be used as a pretext for monitoring of the communications of the person inside the United States.

With respect to the first concern, the PAA actually imposes more judicial oversight than otherwise exists in the standard overseas intelligence collection process by providing the FISC with the jurisdiction to approve or reject the procedures used to determine whether an acquisition constitutes electronic surveillance under FISA. Admittedly, that judicial review is deferential, as it is constrained by the "clearly erroneous" standard of review.

---

[47] The Board believes that the experience of the Terrorist Surveillance Program (TSP), which has engendered controversy precisely because of the debate over whether it complies with the requirements of FISA, reinforces this view.

[48] Vice Chairman Alan Raul is not persuaded by this particular argument.

[49] PAA § 3 (adding Section 105C(b)).

With respect to the second concern, the five conditions the government must certify before it may acquire information pursuant to the PAA limit any broad application of "concerns."[50] Specifically, an acquisition under section 105B may begin only if the DNI and the Attorney General certify, among other things, that the intelligence collection "does not constitute electronic surveillance."[51] Consequently, the government must certify that the acquisition activity either falls outside of the original FISA definitions of "electronic surveillance" or falls within the PAA's exception for surveillance *directed at* a person reasonably believed to be outside the United States. Thus, although these procedures theoretically must ensure only that acquisition does not constitute electronic surveillance, FISA's court-order requirement continues to apply with respect to electronic surveillance directed at persons reasonably believed to be outside the United States.

Board staff met with representatives from DOJ NSD and the ODNI Privacy and Civil Liberties Office regarding the specific classified procedures employed to determine the location of a target and the auditing processes employed to monitor adherence to those procedures. Staff was impressed with the procedures and compliance efforts, as well as the individuals in the respective agencies charged with implementing both elements. Staff provided specific information to the Board in a secure setting.

E. What methods will the government employ to limit any bad-faith behavior on the part of individual analysts?

FISA, as amended by the PAA, requires ODNI and DOJ to monitor compliance with certain surveillance procedures and certifications issued by the Director of National Intelligence and the Attorney General. Both agencies must examine instances where third parties refuse to comply with directives and where government actors fail to comply with the procedures designed to ensure that an acquisition concerns persons reasonably believed to be outside of the United States. As mentioned previously, staff received classified information that reassures the Board that adequate compliance mechanisms exist. The statutes also require the Attorney General and Director of National Intelligence to provide reports of noncompliance to Congress. The Assistant Attorney General for the National Security Division has publicly pledged to provide the relevant Congressional committees with information regarding implementation of the PAA that goes beyond the statutory requirements. The Board recommends that DOJ and ODNI, as a matter of regular procedure, provide as much information as possible (given resource and security concerns) to both Congressional intelligence committees. This information should include (as practical and within the limitations of national security) the number of instances where information has been collected on U.S. Persons through the PAA's amendments and how such information was used.

After conducting its review, the Board concludes that the government appears to be adequately considering the privacy and civil liberties interests of U.S. Persons in the planning for

[50] The Board notes that neither the Director of National Intelligence nor the Assistant Attorney General for the National Security Division could explain during testimony before the House Judiciary Committee exactly why PAA includes the phrase "concerns persons reasonably believed to be outside the United States" at one point as well as the phrase "directed at persons reasonably believed to be outside the United States" in another provision.

[51] *Id*. § 2 (adding Section 105B(a)(2)).

implementation of the PAA. Specifically, it acknowledges the privacy protections built into the protocols surrounding the acquisition of foreign intelligence information, the procedures employed to determine that a person is reasonably believed to be located outside of the United States and the auditing regimes the government has established to promote compliance with all legal requirements. As a general matter, analysts must support their conclusions regarding a target's location, and compliance teams within DOJ's National Security Division and ODNI review those conclusions and other actions on a regular basis. Based on its review of applicable polices, agency practices and training, and new and prior oversight, compliance and audit mechanisms, the Board believes that privacy and civil liberties are being appropriately considered with respect to the PAA.

In addition to the steps the government has already taken to implement the PAA, the Board encourages the National Security Division and ODNI to provide thorough and regular reports to Congress regarding the use of the PAA's provisions. The Intelligence Community will retain the changes made to FISA only if it establishes sufficient trust with lawmakers in Congress and shows that it has used the PAA's authority responsibly. The Intelligence Community may communicate this information and earn this trust by providing to Congress as much specific information as possible, given national security considerations, regarding the intelligence collection efforts authorized pursuant to the PAA. Such information would exceed the reporting mandates contained in the PAA.[52]

Watch List Redress[53]

The Board's 2007 Report to Congress discussed in detail its efforts to facilitate the drafting and execution of a Memorandum of Understanding (MOU) among the ten Federal agencies utilizing terrorist watch list data. At the request of Chairman Dinkins, this initiative was undertaken by Vice Chairman Alan Raul. Those efforts continued into the period covered by this report, and included a meeting with the new Director of the Terrorist Screening Center (TSC) and the TSC privacy officer at the Board's April 26 meeting.

The 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. It works with the National Counterterrorism Center, which serves as the U.S. government's central repository for information on international terrorist identities, known as the Terrorist Identities Datamart Environment (TIDE). The TIDE database includes, to the extent permitted by law, all information the U.S. government possesses on the identities of individuals known or appropriately suspected to be or to have been involved in activities constituting, in preparation for, in aid of, or related to international terrorism.

[52] *Id*. §§ 2, 4.

[53] The Board's efforts on this matter are also noted in a report by the Department of Justice Inspector General (Audit Report 07-XX, September, 2007), available at http://www.usdoj.gov/oig/reports/FBI/a0741/final.pdf (last accessed Sep. 28, 2007). See pp.47, 63, and 66.

The establishment of TIDE marked a major milestone in the Nation's counterterrorism efforts, compiling into one database information on all known and suspected international terrorists. Before 9/11, counter-terrorism watch listing efforts were spread across multiple databases managed by multiple agencies, a significant vulnerability in the Nation's efforts to defend against terrorist attack.

Each day, TIDE sends the TSC a sensitive but unclassified subset of terrorist identifiers to populate the U.S. government's consolidated watch list. This consolidated watch list, in turn, supports efforts to screen, detect, and interdict the travel of known and suspected terrorists here and overseas. These screening efforts encompass the work of consular officers at embassies, Customs and Border Protection (CBP) personnel, law enforcement organizations across the United States, and foreign and domestic air carriers that fly to the United States. So an applicant for a State Department visa is checked against the watch list at a consulate overseas. At U.S. ports of entry, an international traveler's passport, visa, or other valid travel document is also checked against the CBP's subset of the consolidated watch list. And at a routine traffic encounter inside the United States, a suspect's identity is checked against the Terrorist Screening Database through the National Crime Information Center. Finally, airline screening personnel review passenger lists for all flights traveling to the United States to identify individuals who are believed to be a threat to civil aviation or the homeland or who should have additional screening prior to boarding a plane.

Examples of the types of activity warranting an individual's entry into TIDE and terrorist screening systems include:

- Commission of an international terrorist activity;
- Preparation for or planning of international terrorist activity;
- Collection of information on potential targets for international terrorist activity;
- Collection or solicitation of funds or other items of value on behalf of international terrorist organizations or activity;
- Recruitment of members into international terrorist organizations;
- Provision of material support (e.g., safe houses, transportation, communications, funds, false documentation, weapons, or training) to international terrorist organizations; and,
- Membership in or representation of an international terrorist organization.

While the number of names contained in TIDE has grown since its inception in 2003 from approximately 100,000 to over 500,000, this figure represents every identity associated with individuals entered in the database. This distinction is significant because of the multiple aliases and name variants of terrorism suspects. As a result, the number of unique individuals recorded in TIDE is closer to 400,000. Moreover, although TIDE continues to grow, individuals' names are also regularly removed when it is determined that they no longer meet the criteria for inclusion. As a result, more than 10,000 names were removed from TIDE in 2006.

TSC has recently reported that its list "has detected more than 40,000 people trying to gain entry into the U.S. who either associated with terrorist groups or were known terrorists themselves" since the list was created. [54]

The existing TSC watchlist redress process allows 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 terrorism watch list-related. The goal of the redress process was 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.

This 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. TSC has worked closely with screening agencies to establish a standardized process for referral of and response to public redress complaints. It 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 complaints of individuals on the terrorist watch list, evaluate whether such persons were properly listed and that the associated information was correct, and make any corrections which were appropriate, including removal of such persons from the watch list when warranted.

In the fall of 2005, TSC began to document formally the participating agencies' mutual understanding of their obligations and responsibilities arising out of the watch list redress process. Competing priorities and proprietary dispositions concerning information within participating agencies, however, slowed progress. Board intervention in June 2006, however renewed the effort and prioritized the project.

Following a six-month period of negotiations among the participating agencies, in January 2007, a final draft of the MOU was approved and submitted for the signature of the heads of the ten agencies.[55]

The MOU sets forth a 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, to ensure accountability, 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.

---

[54] Sara A. Carter, Terror Data Base Gets Plenty of Hits, Washington Times, October 1, 2007, at A1 (available at http://washingtontimes.com/article/20071001/NATION/110010062/1001 (last accessed Oct. 1, 2007).

[55] MOU signatories agencies include the Departments of State, Defense, Treasury, Justice, and Homeland Security; the Office of the Director of National Intelligence; the Central Intelligence Agency; the FBI; the National Counterterrorism Center; and Terrorist Screening Center.

On September 21, 2007, the Board was notified that the Department of Defense had finally become the last of the ten signatory agencies to execute the MOU. DOD's delay in execution is disappointing in light of the fact that it was represented during the six month period from June to November 2006, in which the MOU working group refined the document to meet all the questions and concerns raised by the signatory agencies. DOD neither raised specific objections to the MOU nor informed the other signatory agencies of reasons for the delay in execution. The Board hoped that with expeditious execution of the agreement, the public could be informed on continuing efforts to enhance redress procedures and the Board working group's attention could turn toward efforts to bring more transparency to the process. That process will now commence, but will have to progress without the assistance of the present Board.

The Board wishes to publicly commend the dedicated efforts of the TSC staff and its privacy officer in working to create a complete and accurate watch list.

FBI Use of National Security Letters

On September 14, 2007, the Board issued a letter to the Attorney General with findings and recommendations concerning the use of National Security Letters (NSLs) by the Federal Bureau of Investigation (FBI).[56]

On March 4, 2007, the Attorney General notified Chairman Carol Dinkins that the Inspector General of the Department of Justice (IG) would shortly issue a report[57] concerning the FBI's use of National Security Letters (NSLs). The Attorney General and Counsel to the President asked the Board to commence a substantive review of the matters raised in the Report. After conducting a full and thorough study of the matter, the Board sent the Attorney General a letter conveying its findings.

In conducting its review, the Board met personally with stakeholders and decision-makers and reviewed the most important primary documents associated with the NSL process. The Board met both with senior FBI officials, including the Director, Deputy Director, and General Counsel, as well as DOJ officials from the National Security Division and the Privacy and Civil Liberties Office (PCLO). The Board also met with the IG and his staff to learn about the concerns and problems identified in the Report. Additionally, the Chairman and Vice Chairman also invited and met with non-governmental representatives of the privacy community, including the Electronic Privacy Information Center and the Center for Democracy and Technology, to discuss their concerns.

In all of these meetings and briefings, Board Members asked whatever questions they desired and received answers to those questions. Board staff was afforded the opportunity to ask additional questions and explore other issues following these meetings. Throughout this review,

---

[56] Board letter to the Attorney General (Sep. 14, 2007), available at http://www.privacyboard.gov/reports/2007/NSLFinal.pdf (last accessed Oct. 1, 2007).

[57] *A Review of the Federal Bureau of Investigation's Use of National Security Letters*, Report of the Inspector General (March 9, 2007), *available at* http://www.justice.gov/oig/special/s0703b/final.pdf (last accessed Apr. 13, 2007) ("Report").

the Board received the support and encouragement of the Counsel to the President to engage in a full investigation and to offer candid recommendations.

As a result of its review, the Board found four issues it felt the FBI needed to address. These concerns include: whether the NSL regime should be altered; whether the FBI should continue independently to manage NSLs; whether the FBI should further reform its internal NSL procedures; and whether there are procedures in place at the FBI to assess when individual employees within the Bureau should be held accountable for the failings identified in the Report.

The Board did not reach any conclusion as to whether Congress should amend the NSL statutes.[58] However, the Board is concerned that the FBI has not made a conscious, direct, and thorough effort to explain to the public and to Congress exactly why NSLs should be retained in their current form. Specifically, it has not made a comprehensive, detailed, and positive argument that NSLs collect essential information in the most timely and effective manner. It has not engaged critics of NSLs with sufficiently detailed information and specific instances of NSL use to allow policymakers to make informed decisions. It also has not described the elements of the current NSL regime that are essential to its operation. Finally, it has not discussed or shown how the current NSL regime appropriately limits risks to the privacy and civil liberties of U.S. Persons. In order to regain support for the use of NSLs generally and to maintain the ability to use NSLs, the Director must explain the benefits and essential characteristics of these tools.

The Board is impressed with the recent steps the Bureau has taken to create a Bureau-wide compliance program seeking to hold individuals accountable for the most egregious violations and instances of noncompliance with regulations and statutes.[59] The Board also believes that, in addition to its internal controls, the FBI should also include Department perspectives and oversight from outside the Bureau in its management of NSLs. Specifically, the Bureau should continue to collect, retain, and disseminate information from NSLs *only* if it shares that responsibility with Department entities and agencies such as the Department of Justice's NSD and PCLO. These offices may share NSL responsibilities with the FBI through strong and regular oversight of the NSL process.[60]

---

[58] Chairman Dinkins recommended to the Board that once reconstituted under Pub. L. 110-53, the new Board membership should interview Federal prosecutors and review the actual usefulness of National Security Letters, including to inquire as to whether grand jury subpoenas are as effective and timely as NSLs.

[59] At the invitation of the Deputy Director of the FBI, Member Frank Taylor coordinated a benchmarking session with relevant Bureau personnel regarding creating and managing compliance programs in the private sector. In early October 2007, Member Taylor and the Board's Executive Director met with the director of the new Compliance Office for a status update of their activities. Member Taylor reported back to the full Board that he was pleased with the Office's progress and the commitment made to it by senior FBI leadership. He also offered his continued personal assistance with private sector compliance experience, following conclusion of the Board's activities no later than January 2008.

[60] The DOJ National Security Division already has begun engaging in such oversight over FBI national security investigations. Specifically, since its establishment, the National Security Division has been building its capacity and increasing the tempo of its oversight activities and, in April 2007, the National Security Division began a regular process of conducting National Security Reviews of FBI field offices and Headquarters national security units. These reviews are staffed by career Department attorneys with law enforcement and intelligence experience from the National Security Division and the FBI's Office of General Counsel, along with officials from the

The Board welcomes the FBI's decision to adopt the recommendations of the IG, including improving the process of tracking NSLs, instituting a policy to require agents to retain copies of signed NSLs, and eliminating the use of "exigent" letters. The Bureau has drafted a series of comprehensive and promising guidelines to implement most of the Inspector General's recommendations. Additionally, as discussed previously, the Board welcomes the FBI's decision to take action beyond the IG's formal recommendations by creating a Bureau-wide compliance program. In addition to the IG's recommendations and the compliance office, the FBI should consider changes to certain internal procedures that likely created or exacerbated the inappropriate use of NSL authorities. *First*, the Bureau should restructure its chain of command to place greater information, control, and accountability in the hands of senior officials and the FBI's Office of General Counsel. *Second*, the Bureau must require agents to compare the information provided pursuant to an NSL against the language of the actual request. *Third*, in evaluating the findings of the Report, the FBI should continue to examine ways to minimize information associated with NSLs in a way that protects the privacy and civil liberties of U.S. Persons and maintains the effectiveness of NSLs.

Finally, the Board believes senior officials in the FBI bear responsibility for failing to create any sort of compliance mechanism prior to the Report and failing to craft procedures to allow information regarding NSL violations to flow to those in authority. Determining exactly what consequences should apply to individual employees, however, requires a careful two-pronged approach. *First*, the FBI or DOJ must determine what took place and who bears responsibility for that action. *Second*, the Bureau must apply those facts to the relevant law, regulations, or internal policies. The Board does not take a position regarding the imposition of any particular penalty or discipline against any particular individual. Rather, it strongly encourages DOJ and the FBI to make such determinations quickly and in as transparent a manner as possible given employee privacy rights.

Department of Defense Threat and Local Observation Notices Program

In the previous report to Congress, the Board discussed its review of the Department of Defense (DOD) Counterintelligence Field Activities' (CIFA) Threat and Local Observation Notices (TALON) program. This review was led by Member Francis X. Taylor. 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. DOD has recently announced that the Deputy Secretary accepted the recommendation of the Under Secretary of Defense for Intelligence to

---

Department's Privacy and Civil Liberties Office. For the first time, DOJ attorneys have been given the clear mandate to examine all aspects of the FBI's national security program for compliance with law, regulations and policies. These reviews broadly examine the FBI's national security activities, its compliance with applicable laws, policies, and Attorney General Guidelines, and its use of various national security tools, such as NSLs. The reviews are not limited to areas where shortcomings have already been identified; instead, they are intended to enhance compliance across the national security investigative spectrum. By the end of this year, the National Security Division will have completed a total of 15 reviews in field offices and headquarters units.

end the program completely effective September 17, 2007. The Board was informed that a record copy of the TALON database is being maintained on compact disk by the CIFA General Counsel for intelligence oversight and Freedom of Information Act purposes.

IV. Policy and Program Review and Analysis Initiated

The Board has undertaken review of several programs since March 1, but subsequently discontinued that review in light of the statutory reconstitution of the Board.

REAL ID Act of 2005

The REAL ID Act of 2005, which was included in the Emergency Supplemental Appropriation for Defense, the Global War on Terror, and Tsunami Relief, 2005,[61] enacts a number of measures and guidelines designed to prevent terrorist acts against the Nation. These measures include updating laws on entry into the country and deportation of terrorists, waiving laws that would impede construction of barriers at the Nation's borders, funding border security protection projects, and changing visa limits for select groups. Most significantly, the Act, as implemented by DHS, effectively requires states to issue new driver's licenses that meet a set of specific Federally-mandated requirements by the end of 2009.[62]

The REAL ID Act requires states to meet Federal standards regarding the supporting documents used to obtain an ID, information required on the ID, and the level of security required to protect collected and stored information. In order to obtain a drivers license, a person is required to give the state government all requested and necessary information. The Act's creation came in response to a 9/11 Commission recommendation for more secure identification.[63] and replaced similar provisions initially passed in the IRTPA. The major difference between IRTPA and the REAL ID Act is that IRTPA's language left many of the minimum standards that apply to the card, as noted above, to be determined by a committee of state and Federal officials. By contrast, the REAL ID Act states that standards are to be set by the Secretary of Homeland Security, in consultation with the Secretary of Transportation and the States.[64]

---

[61] Pub. L. 109-13,

[62] The original law stated a deadline of May 2008, but on March 2, 2007 the Secretary of Homeland Security published a notice providing for states to request extensions to the end of 2009. This came in response to certain amendments to S.4 proposed by Senator Susan Collins, whose home state of Maine opposes the Federal government mandate. Those amendments would have repealed significant portions of the REAL ID Act.

[63] THE 9/11 COMMISSION REPORT, 393-94 (2004), *available at* http://www.9-11commission.gov/report/911Report.pdf (last accessed Nov. 1, 2006). "Recommendation: Secure identification should begin in the United States. The federal government should set standards for the issuance of birth certificates and sources of identification, such as drivers licenses. Fraud in identification documents is no longer just a problem of theft. At many entry points to vulnerable facilities, including gates for boarding aircraft, sources of identification are the last opportunity to ensure that people are who they say they are and to check whether they are terrorists."

[64] "All authority to issue regulations, set standards, and issue grants under this title shall be carried out by the Secretary [of Homeland Security] in consultation with the Secretary of Transportation and the States."

Pursuant to the Act, on March 1, 2007, DHS released a set of proposed rules and minimum standards that would apply to state-issued REAL ID compliant licenses. In response to a request for public comment, DHS received over 21,000 responses. Of particular interest, the DHS Data Privacy and Integrity Advisory Committee (DPIAC) refused to endorse the program and DHS' proposed rules due to a number of omissions and issues that were purportedly "not explore[d] in the depth necessary for a system of such magnitude and such consequence."[65]

As of September 2007, the following states have enacted legislation to either repeal or opt-out of the REAL ID program: [66] Arkansas, Colorado, Georgia, Hawaii, Idaho, Illinois, Maine, Missouri, Montana, Nebraska, Nevada, New Hampshire, North Dakota, Oklahoma, South Carolina, Tennessee, and Washington. Twenty-one additional states and the District of Columbia have similar legislation introduced and pending action.

DPIAC issued 12 recommendations stemming from what its members believe to be omissions from the Proposed Rule (PR). The members would like any Final Rule (FR) to include, for example, explicit steps for security, a redress procedure, limits on what information is collected and how it is used, and a process whereby individuals may access their own personal information. Nearly all their recommendations arise out of concerns that are not addressed in the PR.

1. The FR should set forth an explicit standard for security policies and procedures for states to follow.
2. The FR should list specific steps to prevent unauthorized access to information on the identification card (as opposed to just the state information management systems).
3. The FR should use the American Association of Motor Vehicle Administrators (AAMVA) security program as a foundation for the REAL ID security standard. The AAMV program, among other things, only allows authorized user's access, guarantees the physical security of the technology used, and vets personnel who utilize the data. (Included in the PR)
4. The FR should require states to be accountable for the information they collect and store. Additionally, specific individuals should be named to carry this duty out.
5. The FR should require states to maintain a simple redress procedure and a way for individuals to submit complaints.
6. The FR should require states to provide notices to consumers about the information that is collected and stored and inform them of how it is intended to be used.
7. The FR should take into account that, since persons are required to give consent to their personal information being collected if they are to be able to drive, they cannot refuse to have their data collected in this manner. Because of this, DHS should consider giving

[65] The DHS Data Privacy and Integrity Advisory Committee's Report can be found at http://blog.wired.com/27bstroke6/files/DPIAC_REALID_Submission.pdf (last accessed Sep. 21, 2007).

[66] As reported by the ACLU at http://www.realnightmare.org/news/105/ (last accessed Sep. 21, 2007).

persons the choice of not having their information used for reasons other than law enforcement.

8. The FR should evaluate individuals' access to their own information and ensure such access is available and help is provided to individuals requesting access.
9. The FR should place specific limits on the purpose for which information is collected and used.
10. DHS should consider how easily the Machine Readable Zone on the card, which stores personally identifiable data, may be accessed. The DPIAC suggests the Machine Readable Zone be limited to only include holder's name and address, license issue and expiration dates, and a unique identifier number that can be used to locate the license number on a state system.
11. The FR should require all state drivers license databases to specify restrictions on access, transfer, and secondary uses of information.
12. The FR should require DHS to conduct background searches on employees in state facilities who will be handling production of REAL ID licenses. (Included in the PR)

The Board commends these recommendations for DHS to consider and appropriately address.

Department of Homeland Security Automated Targeting System (ATS)

At the Board's request, on July 16, 2007 the Vice Chairman initiated review of the primary elements of the Privacy Impact Assessment (PIA) and System of Records Notice (SORN) concerning the Automated Targeting System (ATS).[67] He met at the Department of Homeland Security with the Assistant Secretary for Policy and his Deputy Assistant Secretary. It should be noted that ATS is not purely used as an anti-terrorism tool. It helps DHS and CBP fulfill other responsibilities, such as combating smuggling and human trafficking.

ATS actually consists of six separate modules or sub-systems.

- Two modules deal with cargo (one inbound, one outbound);
- One module deals with those who cross the borders via land;
- One module concerns passengers who cross U.S. borders by air, ship, and rail;
- One module collaborates with foreign customs authorities; and
- One module functions as an analytic system.

[67] The SORN was published in the *Federal Register* on November 2, 2006 (71 FR 64543), and the PIA was published on November 29, 2006. Both documents were discussed in a series of Associated Press articles. *See, e.g., U.S. rates travelers for terror risk*, Associated Press (Dec. 1, 2006), *at* http://www.msnbc.msn.com/id/15982036/ (last accessed Jul. 11, 2007). The PIA, SORN, and Notice of Proposed Rule Making for Privacy Act Exemptions were updated based on public comment and the SORN (72 FR 43650) and NPRM (72 FR 43567) were republished in the *Federal Register* on August 6, 2007 . All documents including a response to public comments are available on DHS's web site at http://www.dhs.gov/xinfoshare/publications/editorial_0511.shtm#3.

The land border (ATS-L) and air passenger (ATS-P) sub-systems generated the most public concern and would have the greatest impact on the most number of people. ATS has been screening passengers since the late 1990s, but the collection of data for it has been expanded and automated since the 9/11 attacks.[68] The system applies only to those entering or leaving the United States. It does not apply directly to any forms of purely domestic travel. Although, it does apply to domestic fights preceding or following international flights, when the domestic and international flights are part of a single travel itinerary.

The ATS-P is a rules-based system that does not change from passenger to passenger. Rules are based on current intelligence and change frequently. Examples of rules criteria include, name, age range, profession, and origin or destination of trip. Rules may be quite complex, and even though the number and type of rules that are in effect varies during any given period, the number of individual hits for any given rule is small.

ATS-P does not assign a "score" to passengers. A person is simply a hit or miss (a hit classified as "Augmented Primary") based on the given rule(s) for each day. If a person fits the criteria for any given rule, a screen will alert a CBP Officer and provide additional instructions, including follow up questions the agent should ask the passenger.

ATS is a decision support tool that contains a threshold targeting module. If an individual's travel data elements meet the criteria for a threshold risk scenario, but is not subject to secondary screening, no record is kept of the person's having met the threshold within ATS. Records do result from the process if a traveler is referred to secondary screening for further questioning

ATS-P utilizes a variety of data sources, all listed in the PIA. They include the Advance Passenger Information System, numerous border crossing and visa databases, secondary referral records, personal search records, seized property, and airline passenger name record (PNR) data. ATS-L utilizes DMV data. The system takes the name and license plate of every vehicle coming across the border via car and checks that information with the DMV database for potential threats.

Access to the ATS system is generally limited. CPB Officers who make use of the data are required to undergo privacy training. For the information maintained in ATS (name, risk assessment, rules applied, and PNR), a limited number of users outside of DHS have access to this information. Only if there is a specific information sharing arrangement permitting the development of an outside agency specific rule sub-set will users from that outside agency be permitted to access and review the name, risk assessment, and rules developed for the outside agency. According to the PIA, certain law enforcement task forces and other law enforcement and counterterrorism agencies may issue queries to the system but must have the queries approved by a DHS representative. Outside entities do not have direct access to the system.

The retention period for data maintained in ATS will not exceed fifteen years, after which time it will be deleted, except as noted below. The retention period for PNR, which is contained only in ATS-P, will be subject to the following further access restrictions: ATS-P users will have general

[68] Ellen Nakashima, Collecting of Details on Travelers Documented, *Washington Post*, September 22, 2007, at A1.

access to PNR for seven years, after which time the PNR data will be moved to dormant, non-operational status. PNR data in dormant status will be retained for eight years and may be accessed only with approval of a senior DHS official designated by the Secretary of Homeland Security and only in response to an identifiable case, threat, or risk. Such limited access and use for older PNR strikes a reasonable balance between protecting this information and allowing CBP to continue to identify potential high-risk travelers.

ATS operates independently from already-existing watch list systems and procedures. DHS allows persons, including foreign nationals, to seek access under the Privacy Act to information maintained in ATS, specifically PNR data submitted to ATS-P. And because of the rules-based nature of ATS, individual redress of incorrect or incomplete information is not particularly relevant. According to the PIA, a passenger cannot obtain direct redress of a risk assessment. CBP notes that ATS is a decision support tool that compares various databases, but does not actively collect the information in those respective databases except for PNR. When an individual is seeking redress for other information analyzed in ATS, such redress is properly accomplished by referring to the databases that directly collect that information. Given that an individual may be uncertain what agency handles the information, DHS has set up a redress process DHS Traveler Redress Program (TRIP)[69]. Individuals who believe they have been improperly denied entry, refused boarding for transportation, or identified for additional screening by CBP may submit a redress request through the TRIP. TRIP is a single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs – like airports and train stations or crossing U.S. borders. Through TRIP, a traveler can request correction of erroneous PNR data stored in ATS and other data stored in other DHS databases through one application.

V. A Reconstituted Board

As previously noted, on August 3, 2007, President Bush signed into law the *Implementing Recommendations of the 9/11 Commission Act of 2007*. At the beginning of the 110th Congress, H.R. 1 was introduced into the House of Representatives, and S. 4 was introduced into the Senate. The House passed H.R. 1 on January 9, and the Senate passed S. 4 on March 13. Differences between the bills were not resolved in conference until July 2007, with both Houses of Congress passing the conference report the last week of July.

The present Board questions whether this statute will lead to the intended enhanced status and authority for the Board and its mission, and notes that the initial result was to stall a number of ongoing initiatives and to remove the present Membership and its staff from office. This necessarily requires a new lengthy confirmation process for successors and duplicative efforts by the new membership to educate itself and integrate its operations into those of the Executive Branch.

While the statutory mission remains essentially the same, this act significantly reconstitutes the Board, taking it out of the EOP and making it an independent agency within the Executive Branch. The position of chairman becomes a full time position, and the position of vice

[69] See 72 Fed. Reg. 2294, dated January 18, 2007.

chairman is abolished. All five members must be confirmed by the Senate to staggered six-year terms. The statute does not limit the President's ability to dismiss members at pleasure. The present Board Members may not serve beyond January 30, 2008, and the Board as it is presently constituted ceases to exist.

The reconstituted Board may issue subpoenas for information or testimony from third parties, which subpoenas are enforced by the Attorney General. The statute provides budget authorization beginning with $5 million in FY 2008 and rising to $10 million in FY 2011.

The statute attempts to formalize the relationships between the Board and the various privacy and civil liberties officers throughout the government by, among other things, instituting quarterly reporting requirements. The reconstituted Board itself will report to Congress semiannually rather than annually, and the reports themselves must contain pertinent information on activities, findings, conclusions, minority views, Board advice *not* taken by the Administration, and information on the Attorney General's support of the Board's subpoena authority. With regard to enhanced Congressional reporting requirements, by requiring the Board to reveal its findings, conclusions, recommendations, minority views, and recommendations *not* adopted by the Executive, the legislation makes public the Board's most internal deliberations and communications. These requirements will risk eliminating one of the Board's most effective tools – namely, its ability to operate as a trusted and candid internal adviser within the EOP.

Subjecting all five Members to Senate confirmation, in addition to subjecting the Board to provisions of the Freedom of Information Act (FOIA), triggers the Government in the Sunshine Act, 5 U.S.C. § 552b. This requires the Board to make all of its meetings open to the public with advance notice of its meetings and agendas in the *Federal Register*. Any decision to close a meeting to the public must be made in public and a record of the closed meeting must be maintained. This will likely significantly impede the reconstituted Board's ability to adequately consider issues of a spontaneous or imminent nature.

VI. Issue Recommendations for the Reconstituted Board

The following issues were identified by the Board in its 2007 Report to Congress as worthy of review or on-going monitoring. We recommend that the reconstituted Board assist ongoing review of these programs and issues.

- *Information Sharing Environment (ISE).* As discussed above, the Board is specifically charged with an on-going 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. The establishment of the ISE is coordinated by the ODNI Program Manager. The reconstituted Board should reach out to him and his staff immediately and work to integrate its statutory responsibilities into ISE operations.

- *Government surveillance operations.* The reconstituted Board can 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 reconstituted Board can assist in this process.

- *USA PATRIOT Act and National Security Letters*. The 2006 reauthorization included over thirty new civil liberties protections. The reconstituted Board should work with the Department of Justice to monitor implementation of these protections, and should continue to monitor the development and continuing operations of the new FBI compliance office and the Bureau's use of NSLs.

- *Federal data analysis and management issues*. The reconstituted Board should move quickly to develop a significant understanding of issues associated with data mining activities, data sharing practices, and governmental use of commercial databases. This level of understanding will assist it in review of many Federal anti-terrorism programs. The present Board had been referred the recommendations of the March 2004 report of the Technology and Privacy Advisory Committee to the Secretary of Defense, *Safeguarding Privacy in the Fight Against Terrorism*. The reconstituted Board should review this report and oversee the implementations of its recommendations.

- *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 reconstituted Board should participate in this process.

- *State and local fusion centers*. State and local authorities have created 42 fusion centers around the country. Fusion centers blend relevant law enforcement and intelligence information analysis and coordinate security measures in order to reduce threats in local communities. They also represent a method for providing first responders with *actionable intelligence*; information useful and relevant to the day-to-day mission of state and local law enforcement personnel.[70] According to its web site, as of the end of FY 06, the Department of Homeland Security has provided more than $380 million to state and local governments in support of these centers. Intelligence Officers from the DHS Office of Intelligence and Analysis currently work side by side with state and local authorities at twelve fusion centers. Fusion centers and the two-way information flow accompanying

[70] Testimony of Hugo Teufel III, DHS Chief Privacy Officer, before the U.S. House of Representatives Committee on Homeland Security Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, March 14, 2007.

them require additional effort and vigilance to ensure privacy rights are protected. The *Implementing Recommendations of the 9/11 Commission Act of 2007* directed DHS, in consultation with the Board, to establish a State, Local, and Regional Fusion Center Initiative. In many ways, this initiative is identical to efforts in August 2006 by the Global Justice Information Sharing Initiative, DHS, and DOJ when they collaboratively developed and issued *Fusion Center Guidelines: Developing and Sharing Information in a New Era*. These guidelines were intended to ensure that fusion centers are established and operated consistently, resulting in enhanced coordination, strengthened partnerships, and improved crime-fighting and anti-terrorism capabilities. The reconstituted Board should be included in the continuing development of privacy guidelines applicable to these fusion centers.

- *National Implementation Plan (NIP).* The National Counterterrorism Center is presently conducting the first strategic review of the NIP. The President approved the NIP in June 2006, which for the first time assigned agencies throughout the government specific roles and responsibilities for contributing to the fight against terrorism. The reconstituted Board should study the results of this review and actions taken as a result of its findings and recommendations, and continue to monitor those on-going NIP tasks and activities that might raise privacy or civil liberties concerns.

VII. Conclusion

As the efforts of the current Board come to a close, the Members wish to acknowledge and thank the many thousands of dedicated men and women in the Federal government whose responsibility it is to protect the homeland against terrorism consistent with the Constitution. We have been privileged to observe their training on the importance of privacy and civil liberties and witness their work first hand. The development of a privacy and civil liberties oversight infrastructure within the Federal government, as envisioned by IRTPA, is important. But nothing can substitute for the uncompromising daily commitment these individuals make to their jobs and Constitutional principles.

The Board has also been privileged to play a role in developing the privacy and civil liberties community within the Federal government. Over the past 18 months, the Board established strong working relationships with privacy and civil rights/civil liberties offices in those departments and agencies charged with protecting the homeland. These offices and officers advance privacy and civil liberties at the ground level of their agencies 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 worked most closely include those at DOJ, DHS, ODNI and TSC. These officials have likewise developed lines of communication and authority within their organizations' structure. Their good work will continue and deserves the full support of their agencies.

The relationship between these officials and the Board allowed the Board to encourage the sharing of information and best practices. The relationships also allowed the Board to coordinate and offer assistance when the privacy or civil liberties officers themselves encounter problems. It was a unique relationship facilitated by the Board's placement within the EOP. It will be unfortunate if these relationships cannot easily be duplicated with an independent oversight Board. Nonetheless, the Members of the present Board intend to assist the reconstituted Board in its efforts to organize and initiate activities.

Finally, the Board thanks the President for his confidence and continued support, and for that of the senior members of his Administration. We have appreciated this opportunity to serve the American people in a critical area at this important point in our Nation's history.

Sincerely,

Carol E. Dinkins
Chairman

Alan Charles Raul
Vice Chairman

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