U.S. Department of Justice

THE OFFICE OF PRIVACY AND CIVIL LIBERTIES

2007 ANNUAL REPORT

SEPTEMBER 2007

TABLE OF CONTENTS

I. PRIVACY AND CIVIL LIBERTIES ACTIVITIES

A. NATIONAL SECURITY

This year, the Attorney General tasked the Chief Privacy and Civil Liberties Officer to ensure that the Department of Justice and its components conduct national security investigations with due consideration of the privacy and civil liberties of individuals.

1. National Security Investigations

Following the release of the Inspector General's report on the Department's use of National Security Letters (NSLs), the Chief Privacy and Civil Liberties Officer collaborated with the Assistant Attorney General for the National Security Division (NSD) to examine the issues discussed in the report and provide the Attorney General with a plan to remedy the problems noted. Together they sent a memorandum to the Attorney General summarizing the Department's major actions in response to the Report. As the response notes:

- The Federal Bureau of Investigation's (FBI) Inspection Division began a comprehensive, one-time audit of the use of NSLs in all fifty-six (56) field offices;
- The NSD will conduct regular and ongoing oversight of NSLs;
- The NSD will review all violations reported to the Intelligence Oversight Board (IOB);
- A working group has been convened, co-chaired by the Chief Privacy and Civil Liberties Officer and the Office of the Director of National Intelligence (ODNI) Civil Liberties Protection Officer, which includes members of NSD, the Office of Legal Policy, FBI Office of the General Counsel (FBI OGC), and ODNI, to consider how NSL-related records are used, stored, and disseminated;
- The NSD and FBI considered whether Division Counsel should report to FBI OGC rather than to the Special-Agent-in-Charge of a given Division;

- The Department prepared legislative language to define "toll billing records information," as used in the Electronic Communications Privacy Act (ECPA); and
- The NSD will identify other Department tools and policies that could warrant NSD oversight.

In addition, the Attorney General instructed NSD to report, as part of the IOB process, any significant violations that involve privacy or civil liberties issues. PCLO is working with NSD to define the specifications for the NSD investigators to distinguish situations appropriate for PCLO review in a manner that integrates with current NSD review processes.

In association with the increased oversight, PCLO leadership meets with the FBI Privacy and Civil Liberties Officer on at least a bi-weekly basis to ensure that areas of concern, including the continued development of policy, are addressed in a timely manner. These meetings facilitate the collaborative effort between PCLO and the FBI in enhancing the privacy and civil liberties protections embedded in all the operations of the FBI, not only national security investigations.

2. National Security Letter Working Group

As noted above, at the request of the Attorney General, the Chief Privacy and Civil Liberties Officer for the Department of Justice and the Civil Liberties Protection Officer of the Office of the Director of National Intelligence (ODNI) jointly convened a working group to examine how NSL-derived information is used and retained by the FBI. The group, which included the FBI's Privacy and Civil Liberties Office, Office of General Counsel, and National Security Law Branch, as well as the Office of Legal Policy, the National Security Division, and the ODNI Office of General Counsel, reviewed existing policies and procedures to formulate an enhanced policy that can be implemented by agents in the field and, additionally, enhances the existing privacy and civil liberties protections applied to both information gathering and law enforcement operations in connection with National Security Letters.

The NSL Working Group gathering information on how the FBI handles NSL information.

The working group began with the premise set forth in the Inspector General's report: National Security Letters are critical investigatory tools. The working group then turned to a potential policy option that has been mentioned by various sources: eliminating NSL information upon the closure of a case; however, an examination of the circumstances under which the FBI closes terrorism cases led to the conclusion that the closing of a case was not necessarily indicative of a target's innocence. Additionally, the closing of a case is not determinative of whether or not information gathered during the investigation has current or future investigative value. Thus, to avoid harming national security, the working group believed that controlled retention of information was appropriate.

Further, the FBI informed the working group about enhancements to information technology systems for handling NSL-derived data. Because the new systems provide for the structured storage of information and NSL information can be segregated in the relevant database, the working group concluded that the individual tagging, as that term is commonly understood, of the NSL-derived data did not provide any measurable value for privacy protections at this time. The working group concluded that appropriately labeling and filing information derived from a specific NSL functions as tagging.

Additionally, the working group distinguished the privacy protection needs of the different types of NSL-derived data recognizing the distinctive handling processes and uses for each type. The working group differentiated between "financial and credit data" and "electronic communications transactional data" and developed procedures to address the differences.

The NSL Working Group concluded that significant limitations, which protect privacy and civil liberties, already exist governing the proper use of NSLs and are set forth in terms of the applicable statutes and guidelines. For example, an NSL can only be used in order to gather information that is relevant to a national security investigation. NSLs cannot be used to gather information during the course of a general criminal investigation or a domestic terrorism

investigation. Moreover, an NSL can only be issued with the approval of a high-ranking government official who is charged with reviewing the connection between the information sought and the investigation, to ensure that the material sought is, in fact, likely to be relevant to the investigation. Furthermore, the government can only obtain limited information with an NSL, some of which may be publicly available (e.g., telephone subscriber information). Together, these limitations "minimize" the collection of U.S. person information providing privacy and civil liberties safeguards.

From these findings, the working group reviewed and edited a proposed directive from the FBI's Privacy and Civil Liberties Office and the FBI OGC's National Security Legal Branch (NSLB). The developed data minimization directive assists with both ECPA derived information and Fair Credit and Reporting Act derived information. The working group worked with the FBI to provide guidance documents as well, including a checklist, for agents to reference during investigations to ensure proper application of the policy under this directive.

3. National Security Reviews

The Office of Privacy and Civil Liberties, working with the Office of Intelligence Policy and Review and the FBI National Security Legal Branch, has begun to examine the policies and procedures employed by the Department and the Federal Bureau of Investigation regarding the application of intelligence collection in counterterrorism and counter-intelligence activities to ensure appropriate protections for privacy and civil liberties through National Security Reviews (NSRs). Upon reviewing the activities of the agents in the field using intelligence tools during the investigative process, PCLO will further advise the Attorney General on how to enhance the protections for privacy and civil liberties.

In June, a new Deputy Privacy and Civil Liberties Officer with extensive privacy and operational experience was brought on to represent PCLO as a participant in the onsite reviews at FBI regional offices as part of this process. Not only is PCLO reviewing the actions taken during investigations, but it is also assisting in ensuring that the reviews capture the full picture to permit the

Department to develop enhanced policies and procedures to implement appropriate protections and safeguards while at the same time ensuring that the right information gets to the right person at the right time.

Further, PCLO began to look at the internal mechanisms associated with information collected in the course of protecting the Nation from harm. The review will provide a fair and equitable application of appropriate privacy protections to both information gathering and law enforcement operations. Only through working closely with the persons assigned to provide these essential protections can we develop integrated policies and procedures that robustly promote privacy and civil liberties while at the same time not discounting the important work done by law enforcement and homeland and national security analysts to identify threats and act upon them properly.

4. President's Privacy and Civil Liberties Oversight Board

Throughout these activities, PCLO coordinated with the President's Privacy and Civil Liberties Oversight Board to ensure that the Board was fully informed about the issues presented as well as the proposed corrective actions. The Board provided important additional insight into the merger between national security issues and the protection of privacy and civil liberties. The Chief Privacy and Civil Liberties Officer met regularly with the Executive Director of the Board and kept the entire Board briefed on the topics of interest. Many of the recommendations from the Board supported the conclusions of PCLO and were or will be incorporated into Departmental policies to enhance the existing privacy and civil liberties safeguards.

B. INFORMATION SHARING

At the end of 2006, the President approved for issuance and implementation, and the Information Sharing Environment Program Manager (ISE/PM) released to the public, the Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment, also known as the "ISE Privacy Guidelines." This was the work product of the working group that the Department's Chief Privacy and Civil Liberties Officer co-chaired with the Civil

Liberties Protection Officer of the Office of the Director of National Intelligence to formulate useful guidance, in consultation with the President's Privacy and Civil Liberties Oversight Board, pursuant to Guideline 5 of the President's Memorandum to the Heads of Executive Departments and Agencies on the Guidelines and Requirements in Support of the Information Sharing Environment (ISE), dated December 16, 2005. As such, the ISE Privacy Guidelines implement the requirements of the Intelligence Reform and Terrorism Prevention Act and Executive Order 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans.

1. Privacy Framework

The ISE Privacy Guidelines provide the framework for enabling information sharing while protecting privacy and other legal rights. To achieve this, the ISE Privacy Guidelines strike a balance between consistency and customization, substance and procedure, oversight and flexibility. These guidelines build upon existing resources within executive agencies and departments for implementation.

The ISE Privacy Guidelines require departments and agencies to designate an "ISE Privacy Official" with agency wide responsibility for information privacy issues, to directly oversee implementation of the guidelines. Additionally, the ISE Privacy Guidelines direct the establishment of an ISE Privacy Guidelines Committee (ISE/PGC), consisting of the ISE Privacy Officials of the departments and agencies comprising the Information Sharing Council (ISC) and chaired by the Program Manager. The ISE/PM designated the Department's Chief Privacy and Civil Liberties Officer and the Civil Liberties Protection Officer for the Office of the Director of National Intelligence to serve as co-chairs of the ISE/PGC. Since the issuance of the ISE Privacy Guidelines, this committee has worked on various issues attendant to the implementation of the Guidelines on an agency level. Additionally, the co-chairs coordinated this effort with the President's Privacy and Civil Liberties Oversight Board to ensure appropriate review of the application of privacy and civil liberties safeguards.

2. Implementation Guidance

To provide agencies with further guidance on the practical application of implementing the ISE Privacy Guidelines, the ISE/PGC established various working groups which include the Model Privacy Policy Implementation Plan working group, the Legal Issues Ad-Hoc working group, the State/Local/Tribal governments working group, the Civil Rights/Civil Liberties working group, the Training and Outreach working group and the Foreign Partners working group. In this regard, PCLO participated in a number of the working groups, including the legal ad-hoc working group, which provided the majority of the legal interpretation of the core privacy principles affecting the government's information sharing efforts. For example, this working group has developed tools for agencies to comply with and implement disclosure mechanisms necessary under the Privacy Act for the sharing of ISE information, as well as practical tools for agency application of data quality, data security, notice, and redress policies.

Additionally, PCLO contributed substantially to other ISE/PM working groups established to handle ISE issues. These include ISE Guideline x working group on Controlled Unclassified Information (otherwise known as Sensitive But Unclassified information) and a working group devoted to developing policy and procedures for Suspicious Activity Reporting.

C. INTERNATIONAL ACTIVITIES

The Office of Privacy and Civil Liberties recognized the importance of engaging with the Department's international partners on privacy and civil liberties issues to supplement the Department's already strong national security and law enforcement ties. Through these outreach activities, PCLO worked to help our international partners understand the United States' privacy framework, identifying shared interests and explaining the fair information principles espoused within U.S. privacy law.

1. High Level Contact Group

At the November 6, 2006 Justice and Homeland Affairs Ministerial, the United States-European Union High Level Contact Group (HLCG) on data

privacy and law enforcement cooperation was created. The Chief Privacy and Civil Liberties Officer represented the Department of Justice's interests. The overall intent of the group is to articulate a common set of principles that will improve and harmonize information sharing in the areas of law enforcement and public security.

In the past few years, tension has arisen between the U.S. and EU regarding the different privacy rules that govern information sharing between the parties. Issues such as the Passenger Name Record data transfer have highlighted the misunderstandings of each government's privacy framework. Officials from both governments established the HLCG to explore how the U.S. and the EU could agree on common principles of data protection, but without defining a specific final product in order to provide flexibility during the negotiations. Additionally, the HLCG was not formed to force particular positions or policy on one or the other government. Rather, officials recognized that much of the rhetoric concerning privacy belied an underlying commonality, which was lost in the translation between U.S. jurisprudence and EU law.

Earlier this year, the U.S.-EU High Level Contact Group identified a number of potential principles pertinent to transatlantic cooperation in the area of justice and home affairs. The Chief Privacy and Civil Liberties Officer led an Experts' Group that was established to conduct an ongoing review of the principles, which combine data privacy principles common to the U.S. and EU in order to form an agreed upon set of principles for law enforcement purposes, border enforcement, and public and national security.

The various authorities within each group's jurisprudence contain common elements establishing the core tenets for the privacy rights of individuals concerning the government's collection, use, dissemination, and maintenance of personally identifiable information. Principles such as purpose specification and use limitation as well as data quality and integrity can be found not only in the U.S. Privacy Act, but also within the EU Data Protection Directive.

The HLCG demonstrates that open communication to explain underlying and core rules concerning privacy can lead to international harmonization of privacy supporting frameworks.

2. PNR Negotiations

The Chief Privacy and Civil Liberties Officer represented the Department during the U.S. government negotiations concerning the transfer of and access to passenger name record information. In May 2006, the European Court of Justice held that the original compact agreed to by the Department of Homeland Security, through its Customs and Border Protection component, and the European Commission was not appropriate given the subject matter of the underlying undertakings and that a new agreement must be completed by September 2006. Although a final agreement was not reached until May 2007, an interim agreement was entered into in September 2006, meeting the court's requirements.

The Chief Privacy and Civil Liberties Officer provided advice and counsel to the negotiating team concerning privacy issues surrounding European data protection law. Although the Department of Homeland Security was the lead agency concerning the new agreement, particular national security and law enforcement issues surrounding the collection of passenger name record data necessitated the Department's involvement. PCLO provided core Privacy Act advice and counsel not only to the Department of Justice members of the negotiating team, but to the members from other federal agencies as well.

D. PRIVACY SENSITIVE TECHNOLOGIES

1. Biometrics

PCLO participates actively in examining the privacy issues attendant to the use and deployment of biometric technologies, including as a member of the National Science & Technology Council's Subcommittee on Biometrics. Currently, PCLO co-chairs the Social, Legal, Privacy working group with the DHS Privacy Office. The working group developed a Privacy and Biometrics paper that provides an overall awareness of the privacy issues associated with biometrics, including the issues surrounding the initial collection, enrollment of

individuals into a biometrics system, and the sharing of biometric data both with other federal agencies and international/domestic law enforcement partners. The working group is currently developing a government-wide operational guide for integrating privacy protection into the design of biometric systems.

Additionally, PCLO serves on legal issues working groups for other biometric efforts in the Department and the U.S. government to provide legal counsel and policy advice concerning appropriate safeguards for privacy and civil liberties.

2. Data Mining

PCLO works with the Department and its components, including the FBI, to ensure that the Department deploys data mining technologies in a manner that appropriately protects privacy and civil liberties. Any new information technology system will be reviewed through the privacy compliance process, which includes a Privacy Impact Assessment, to address how the particular deployment of the technology impacts the privacy and civil liberties of individuals.

Pursuant to the requirements of the USA PATRIOT Improvement and Reauthorization Act of 2005, in July of 2007 the Department issued a report to Congress on pattern-based "data mining" activities by the Department and its components. The report outlined six different initiatives at the FBI that qualify as pattern-based data mining activities under the Section 126 of the law:

1. The Identity Theft Intelligence Initiative examines and analyzes consumer complaints about identity theft in order to identify commonalities that may be indicative of major identity theft rings in a given geographic area. The initiative helps identify possible offenders who are the subject of multiple, similar consumer complaints in a given geographic area. This initiative has been used to identify major identity theft trends and organizations as well as generate leads for FBI field offices since 2003.
2. The Health Care Fraud Initiative examines summary health care billing records in government and private insurance claims

databases to help the FBI identify anomalies that may be indicative of fraud or over-billing by health care providers Introduced in 2003, this initiative has resulted in the initiation of more than 50 FBI investigations and nearly 200 referrals to state and local and other federal agencies, resulting in numerous criminal convictions and civil settlements for violations of health care fraud statutes.

3. The Internet Pharmacy Fraud Initiative examines consumer complaints to the Food and Drug Administration about fraud by Internet pharmacies to develop common threads that may be indicative of larger fraud by such pharmacies. The initiative performs analysis that FBI agents used to perform manually in order to improve the investigation and prosecution of Internet pharmacies involved in illegal activities.

4. The Housing Fraud Initiative examines public source data on real estate transactions to identify potential indications of fraudulent housing purchases. First completed in 1999, this FBI initiative has proven effective at identifying real estate transactions likely to be fraudulent in a given area, especially in situations where the same lenders and brokers are consistently associated with a similar fraudulent process (commonly known as "property flipping)."

5. The Automobile Accident Insurance Fraud Initiative compares information on possible fraudulent insurance claims provided by the National Insurance Crime Bureau against other data to identify the national scope of staged accident frauds; to identify major perpetrators and organized groups; and to identify multi-city clusters where staged accidents are occurring. This FBI initiative is only in use in one field office, but plans are in place for larger deployment.

6. The System-to-Assess Risk (STAR) Initiative, which is not yet operational, will be designed to help FBI analysts prioritize the risks associated with individuals who have already been identified as persons of interest in connection with a specified terror threat.

> The initiative will not label anyone a terrorist, but is designed to save time in helping to narrow the field of individuals who may potentially merit further scrutiny with respect to a specific terrorist threat.

Each of the six data mining initiatives discussed in the report is subject to numerous federal statutes, as well as strict Department policies and regulations designed to protect the privacy and civil liberties of Americans.

In connection with the examination of these programs, it was noted that pursuant to Attorney General Guidelines, no investigative activity is initiated by an FBI field office against any individual through any data mining initiative unless the criteria established in the Attorney General Guidelines is met, which includes the logical evaluation of the lead information through other non-intrusive, lawful means. In addition, the use of more intrusive techniques (grand jury subpoenas, administrative subpoenas, tasking of sources, undercover operations, and electronic surveillance) is regulated by law and procedures designed to ensure that the techniques are lawfully and appropriately employed.

At the Department, data mining technologies are typically deployed as a decision support tool and are only one part of an extensive toolkit employed by an analyst or agent in carrying out national security or law enforcement duties.

PCLO recognizes its unique role in monitoring the use of technology and its impact on privacy and civil liberties and will continue to work with the Office of the Chief Information Officer and the Department's components to develop departmental guidance for data mining activities. Although Department programs that use data mining tools and technologies also employ traditional privacy and security protections, such as Privacy Impact Assessments, Memoranda of Understanding between agencies that own source data systems, privacy and security training, and role-based access, PCLO will also work to educate the Department components on how to apply appropriately privacy protections to data mining programs and will monitor the implementation of appropriate safeguards addressing the privacy concerns raised by data mining.

II. PRIVACY COMPLIANCE OPERATIONS

A. PRIVACY ACT

The Office of Privacy and Civil Liberties continued its role of advising the Attorney General on the appropriate privacy protections relating to the collection, storage, use, disclosure and security of personally identifiable information held by the Department. To accomplish this, PCLO serves as the primary point of counsel for the Department on issues relating to the Privacy Act of 1974 and the application of the fair information principles throughout the Department.

1. Maintaining "Systems of Records"

In order to carry out the Department's important and varied law enforcement missions, the Department must handle and maintain a certain amount of information about individuals. The information that the Department maintains about individuals ranges from information within the federal prison system, to information related to cases in litigation, to investigative law enforcement files. The Privacy Act represents the embodiment of a code of fair information principles that governs the collection, use, dissemination, and maintenance of information about individuals that is maintained in "systems of records" by federal agencies. A "system of records" is a group or collection of records under the control of a federal agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual.

In order to ensure that the Department continues to comply with the Privacy Act, PCLO works on a number of fronts. Primarily, PCLO advises components by providing Privacy Act legal analysis and interpretation as it applies to the Privacy Act information held by the Department. In this role, PCLO advises components interpreting the Privacy Act through case law and OMB guidance in order to assist components in the performance of their daily agency operations and functions while continuing to protect the rights of individuals from unwarranted invasions of personal privacy. This is a core principle of the Privacy Act that the Privacy Act evidences through a general prohibition on the disclosure of information about individuals from a system of

records absent written consent of the subject individual, unless the disclosure is pursuant to one of the twelve statutory exceptions.

2. Legal Counsel

In addition, PCLO counsels components regarding Privacy Act implications in connection with litigation and legislative issues; develops and conducts Privacy Act training; and provides guidance on Privacy Act regulations. Furthermore, PCLO works on many interagency efforts in connection with the Privacy Act. For example, PCLO drafted and promulgated a routine use to implement recommendations from the President's Identity Theft Task Force to ensure appropriate capability for response in the situation of an actual or potential unauthorized disclosure of personally identifiable information. This routine use was added, as appropriate, to the Department's systems, 72 Fed. Reg. 3410 (January 25, 2007), and was used as the model for other agencies to comply with the Task Force's recommendations.

3. Statutory Notices

In addition to the wide-ranging general Privacy Act duties of PCLO, PCLO also assists components in developing appropriate language for the required notices to ensure compliance with the Privacy Act. The System of Records Notice (SORN), provides the public with the essential details about a system of records, including the purpose for its operations, the categories of individuals affected by its operations, the categories of information to be used and collected by the agency, where the agency maintains the information, what means of access and correction are available to the individual, what security measures safeguard the information, and, lastly, although very importantly, with what entities and under what conditions the agency will share the information in the system. PCLO counsel address issues related to both new systems and updates to existing systems to develop the appropriate notice to the public concerning Department of Justice systems of records.

In addition to its extensive work with SORNs, PCLO also provides input in connection with Privacy Act Statements, which are notices provided to the public when the agency collects personally identifiable information. These

notices reiterate some of the information found in the SORN, but are designed to provide an individual with certain information at the time he or she provides the information to the agency. The notices must inform the individual of the authority for the collection of the information and whether disclosure of such information is mandatory or voluntary; the principal purposes for which the information is intended to be used; the circumstances under which the information may be shared outside the agency; and the effects on the individual, if any, of not providing all or any party of the requested information. Additionally, if the collection involves Social Security Numbers, the Privacy Act, under Section 7, requires the agency to inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority the Social Security Number is solicited, and what uses will be made of it.

B. E-GOVERNMENT ACT AND FISMA

The Office of Privacy and Civil Liberties serves as the focal point for the approval process for Privacy Impact Assessments (PIAs). In March 2007, Department of Justice Order 3011.1A was modified to reflect the transition of responsibility concerning the approval of PIAs from the Office of the Chief Information Officer to PCLO. Although the PIA process continues to be a highly collaborative process working with the Department's Chief Information Officer, the modification of the order reflects the appropriate placement of authority and responsibility to permit the Chief Privacy and Civil Liberties Officer to ensure appropriate privacy protections for personally identifiable information maintained in the Department's existing or proposed information technology and information systems. Shifting responsibility to the Chief Privacy and Civil Liberties Office also permits effective oversight of the implementation of appropriate policies and procedures, including appropriate training and auditing, to ensure the Department's compliance with privacy-related laws and policies, including Section 208 of the E-Government Act.

1. PIA Process

As discussed above, conducting a PIA at the Department is a highly collaborative process that incorporates the information technology know-how of

the Office of the Chief Information Officer and the privacy compliance expertise of PCLO.

PCLO developed a PIA Manual for use by the Department in determining when a PIA is required, what information should be included in the PIA, and advice on writing the PIA. To simplify the writing of a PIA, PCLO created a template that is used by the Department system owners to submit the PIA. Additionally, PCLO developed a Privacy Threshold Analysis (PTA) template specifically tailored for Department systems and processes. PCLO is currently in the process of updating these documents. Furthermore, PCLO maintains a listing of completed PIAs (available online at http://www.usdoj.gov/pclo/pia.htm).

In addition to the general PIA process, PCLO and OCIO have embedded the PIA process into the overall accreditation process for information technology systems at the Department by incorporating the PTA requirement into the software application used to track compliance with the Federal Information Security Management Act (FISMA). The submission of a PTA is a requirement of the certification and accreditation (C&A) process, which requires program managers for information technology systems, either in development or operation, to evaluate security controls to ensure that security risks have been properly identified and mitigated. All information technology systems must receive a minimum score to be certified and accredited and get their authority to operate (ATO). Including the PTA in this process not only assists in identifying information assets requiring appropriate security controls, but it also permits better identification of those Departmental systems that contain personally identifiable information, thereby identifying for PCLO those information technology systems that require PIAs.

Once an information technology system is determined to require a PIA, the full PIA process involves a coordinated effort between the OCIO and PCLO to produce a final approved PIA.

The PIA review and approval process begins with the examination of the PIA to ensure that the submitting component addresses all of the various questions and requirements within the PIA template. The next stage ensures that

the submitting component provides the information necessary to permit a full evaluation of the risks to individual privacy associated with the operation of this information technology system. The OCIO and PCLO work closely with the system owner to extract the pertinent knowledge required to do the full analysis. At this point, the component privacy office usually participates as part of the informational evaluation.

Once this informational review completes, the next stage is an evaluation of the analytical aspect of the PIA. This process looks to understand from the description of the system and the personally identifiable information involved the impact that this information technology system will have on the individual.

The evaluation begins by asking a number of operational questions:

- What information is to be collected?
- How will be it stored, managed, and used?
- What means of individual access is available?
- How does the system address any implicated constitutional concerns?
- What means of redress for informational errors has been provided?
- What safeguards are in place to protect the information?
- What methodology was employed to develop the system?

This analytical step involves the OCIO, the component privacy office, and PCLO and many times produces inquiries that drive design changes into the development of the information technology system.

Once the analytical review finishes, PCLO takes on the in-depth privacy review to ensure alignment with Departmental policy and guidance concerning appropriate safeguards for privacy and civil liberties. This review addresses more specific privacy concerns, such as use and incorporation of Social Security Numbers within a system, whether or not the operation of a system will require a new Privacy Act System of Records, or issues concerning OMB mandates for privacy protections. After the system manager fully addresses these issues, then the PIA is presented to the Chief Privacy and Civil Liberties Officer for approval with the recommendation of the CIO and PCLO staff.

In addition to looking at the traditional areas covered by a PIA, PCLO and the FBI's Privacy and Civil Liberties Office worked together to look into how to enhance PIAs to cover civil liberties issues. Although a close connection exists between privacy and civil liberties, considering the Department's primary role as the lead law enforcement entity in the United States, special consideration of civil liberties concerns was seen as appropriate. Working together, the FBI PCLO and PCLO developed a number of preliminary questions that will be incorporated into a new version of the PIA guidance and template.

2. PIA Training

In the past year, PCLO conducted training on the Department's PIA process to instruct system owners and project managers on the import and application of the PIA process to the overall development of information technology systems. Many Department of Justice personnel attended the session; PCLO intends to make this training available periodically in order to provide necessary drafting assistance as well as a base understanding of appropriate privacy protections.

In addition to this particular event, PCLO worked with the Office of the Chief Information Officer to enhance the Computer Security Awareness Training (CSAT) module that each employee or contractor with access to Department information technology resources must complete on an annual basis. The update to the training highlighted three key additions to the existing privacy aspects of the training. First, it made Department employees and contractors aware that the Department maintains processes to respond to privacy incidents surrounding the loss, or even potential loss, of personally identifiable information. Next, it highlights additional instances when PII handled in connection with Departmental systems. Last, it enhanced the Rules of Behavior provided at the close of the training to emphasize the individual's as well as the Department's responsibility concerning the protection of PII.

3. FISMA and E-Government Act Reporting

PCLO is responsible for preparing quarterly FISMA privacy reports required by OMB. These reports build on the PTAs and PIAs prepared by the

Department and help the PCLO to confirm the number of IT systems in the Department that collect personally identifiable information, that require PIA and Privacy Act documentation, and for which such documentation has been completed. To aid in the collection of this information, PCLO worked with OCIO to develop the capability within the software application that tracks FISMA compliance to capture relevant privacy information and documentation.

The information in the quarterly FISMA privacy reports is also used by PCLO to determine the Department's and components' privacy compliance as measured by the President's Management Agenda scorecard. PCLO determines if a component will receive a passing grade, and if not, will inform the component what it must do to remedy the problem by the next quarter.

PCLO also reviews and provides a score for the privacy portion of every Department OMB 300 business case before it is submitted to OMB.

4. Privacy Committee

In addition to its internal activities, this year PCLO volunteered to co-chair with OMB the new Privacy Committee under the CIO Council to provide an inter-agency forum for Senior Agency Officials for Privacy (SAOP) and work to develop guidance under the E-Government Act. PCLO did this in recognition that many of the lessons learned through the internal process would provide useful knowledge to other agencies and that PCLO would be privy to new facets of thinking in applying appropriate privacy protections that it could use to inform its own decisions. Currently, this Committee is being formally stood up by OMB and one of the first tasks that PCLO chose to undertake was to create a small working group, which includes privacy officials from the Department of Homeland Security, the Federal Trade Commission, the National Institute of Standards and Technology, the Department of State, the United States Postal Service, and the Office of the Director of National Intelligence, to examine the definition for "personally identifiable information." While this project is still in its earliest stages, it does show great potential to remove the inconsistencies that have existed in different agency interpretations of the term and provide a focused, unified definition for application.

III. OUTREACH AND INTERGOVERNMENTAL ACTIVITIES

To further its mission, PCLO conducted numerous outreach activities explaining the impact of its activities on privacy and civil liberties. TPCLO interacted with outside organizations, including privacy and civil liberties advocates and organizations. Additionally, PCLO worked with individuals to address issues concerning the impact that Departmental activities had on privacy and civil liberties.

A. EVENTS AND TALKS

The Chief Privacy and Civil Liberties Officer spoke at a number of events describing the integration of privacy and civil liberties protections into the mission of the Department. Such events included speaking to the Global Privacy and Information Quality Working Group (GIPIQWG) on Privacy Issues Across Federal Partners and to the American Society of Access Professionals, on security and associated privacy issues from an information technology perspective.

This outreach extended to the international arena. The Chief Privacy and Civil Liberties Officer participated as an observer at the spring 2007 meeting of global privacy and data protection commissioners. Although this conference has closed sessions for only those commissioners providing oversight over all of their country's activities, including commercial data protection, the Chief Privacy and Civil Liberties Officer was granted observer status to all closed sessions in recognition of PCLO's impact on privacy and civil liberties issues. The international outreach continued with participation at the Consortium on EU/U.S. Cooperation in Athens, GA.

B. PRIVACY LEADERSHIP

In addition to speaking about privacy and civil liberties safeguards, PCLO works with different governmental groups on multiple levels to help build an understanding of the government's responsibility in ensuring the privacy and civil liberties of individuals. This work extends not only to collaborating with other federal agencies, but with state and local entities and officials.

In connection with the President's Privacy and Civil Liberties Oversight Board (PCLOB), PCLO participated in collaborative discussions with the other

statutory privacy and civil liberties officers in the federal government from agencies with national and homeland security responsibilities. The Chief Privacy and Civil Liberties Officer met with the Executive Director of PCLOB, the Chief Privacy Officer and Civil Liberties and Civil Rights Officer of the Department of Homeland Security, and the Civil Liberties Protection Officer of the Office of the Director of National Intelligence. These meetings provided each agency's privacy and civil liberties leaders an opportunity to share ideas not only to enhance internal privacy and civil liberties safeguards, but also to build bridges between operational aspects of the agencies in a manner that took into account privacy and civil liberties.

Beyond this group of privacy and civil liberties leaders, the Chief Privacy and Civil Liberties Officer participated in a number of working groups that address various operational and mission related concerns for differing entities. As mentioned above, the CPCLO is co-chair of the Privacy Committee of the CIO Council to deal with harmonizing privacy guidance for federal agencies. Additionally, the CPCLO participates with the Global Advisory Committee to ensure privacy and civil liberties safeguards become embedded in the framework of information sharing concerning the sharing of law enforcement information. Furthermore, the CPCLO's placement as an Associate Deputy Attorney General in the Office of the Deputy Attorney General, ensures that policy and management decisions that affect the entire Department receive appropriate counsel on privacy and civil liberties concerns.

C. PRIVACY AND CIVIL LIBERTIES COMPLAINTS

The Office of Privacy and Civil Liberties assisted the Department in addressing various complaints received concerning the impact of Departmental activities on privacy and civil liberties. This assistance ranged from requests for assistance in seeking access to information to providing legal counsel on Privacy Act issues to supporting legal actions undertaken by the Department.

PCLO facilitated general requests for assistance by directing individuals to the appropriate component or program that either held the information sought by the individual or operated the program or system that impacted the individual. To that end, PCLO developed close relationships with different

offices throughout the Department and in particular with the Civil Rights Division through PCLO's participation in the bimonthly meetings that Division holds with members of various communities impacted by the Department, government, or law enforcement activities.

In connection with requests for information by individuals, PCLO works very closely with the Office of Information and Privacy, which is the federal government office with the lead for Freedom of Information Act and governmental record disclosure actions. The Freedom of Information Act, through the appropriate disclosure of records held by the government, ensures transparency of government actions, and provides a mechanism for individual access to federal records that often interfaces with the Privacy Act's access provision.

IV. CONCLUSION

The Office of Privacy and Civil Liberties is an effective and important partner at the Department in developing policies and procedures that enhance privacy and civil liberties safeguards in Departmental programs and in carrying the message to other federal, state, local and international colleagues that privacy and civil liberties safeguards are an important and necessary part of any initiative.

PCLO will continue to work to ensure that privacy is woven into the very fabric of the Department as a guiding principle and value so that the Office's influence is felt outside the walls of the Department, both at home and abroad, by listening to privacy concerns and by responding in positive, constructive ways.

In addition, PCLO will endeavor at all times to keep an open door to the privacy and civil liberties community around the Nation and the world to ensure that the Department benefits from the range and depth of knowledge and experience of privacy practitioners and concerned citizens everywhere.

PCLO and the Department face great challenges by seeking to achieve both security and privacy and, with both, sustain our values and freedoms.

As such, PCLO will continue to move forward together and achieve the Department's mission of protecting and defending the lives and way of life of the people of this Nation, preserving the Liberty promised in the Constitution, and, with it, the privacy and civil liberties of individuals. The framers of this Nation's Constitution thought privacy and security were compatible ideas. They spoke of Justice, domestic Tranquility, a common defense to promote the general Welfare, and, perhaps most significantly, they spoke of securing the Blessings of Liberty. It is the great hope and, indeed, great belief of the Office of Privacy and Civil Liberties, and the Department of Justice, that we will ensure domestic tranquility and secure the blessings of liberty to ourselves and our posterity.