# 2009 Annual Report for Privacy

*(Covering periods 2007-2009)*

**March 31, 2010**

***[An electronic copy of this report is available at www.treas.gov/foia/privacy]***

## Message from the Chief Privacy Officer

Daniel Tangherlini
*Assistant Secretary for Management*
*and Chief Financial Officer*
*Department of the Treasury*

In response to Section 522 of the Consolidated Appropriations Act of 2005, I am pleased to present the Department of the Treasury's 2009 Annual Report for Privacy. Over the past few years, Treasury's privacy program has undergone a number of structural changes. Because this is the Department's first report since these changes have occurred, this report will cover periods from FY 2007 through FY 2009, with a look into FY 2010. The report contains three primary sections that describe the past, present, and future of privacy at the Department of the Treasury.

Section I, entitled "Privacy in the Past", reflects on the history and re-organization of privacy within the Department, particularly activities from 2007 through 2008. The continual need to safeguard and protect personally identifiable information (PII) grew beyond the protections of the Privacy Act of 1974, and caused the agency to establish a number of new milestones. As discussed in this Section of the report, the chief organizational milestone was the realignment of privacy functions and the creation of the Office of Privacy and Treasury Records (OPTR), which includes the Office of Privacy and Civil Liberties (OPCL). Most notably, the strategic re-alignment that created OPTR elevated privacy-related activities within Treasury bureaus and raised the privacy and data protection profile to a major Department-level initiative. As such, activities such as streamlined compliance reporting, privacy awareness training, and PII incident handling have a much greater impact and have already produced an even greater effect.

Section II, entitled "Privacy in the Present", highlights major activities and accomplishments in 2009. In the Department's efforts to maintain transparency and open government, there have been increasing demands to disclose more information to members of the public and to share data with other Federal agencies. As a result, the Department continually seeks to strengthen its requirement to safeguard PII through its written policies and procedures. This Section discusses the Department's progress on the various checks and balances that support this effort, such as the drafting of System of Records Notices (SORNs) and Privacy Impact Assessments (PIAs), which are monitored by reporting mechanisms, such as the Federal Information Security Management Act of 2002 (FISMA) and Section 803 of the Implementing Recommendations of the 9/11 Commission Act. This Section also focuses on the Department's intra-agency and interagency efforts to improve the quality and efficiency of privacy safeguards within the Federal Government.

Section III, entitled "Privacy in the Future", provides information on 2010 privacy initiatives in the Department. In response to a new Directive on open government, Treasury Privacy and Information Technology (IT) offices will explore the technological advances of Web 2.0 applications and cloud computing. We will continue to monitor the Department's compliance with existing statutes, mandates, and regulations. In 2010 and beyond, we will strive to ensure that policies dictating web-based activity contain the appropriate technical, physical, and administrative safeguards needed to protect PII and other protected data.

## Table of Contents

# I. Privacy in the Past (2007-2008)

## A. Historical Overview

On October 2, 1975, the Secretary of the Treasury issued regulations implementing the Privacy Act at 31 CFR Part 1, Subpart C. Treasury Directive (TD) 25-04, "The Privacy Act of 1974, As Amended," [1] established guidelines and assigned responsibilities for carrying out the requirements of the Act. This TD is presently being revised to include a key privacy function—"redress"—for which Treasury's Senior Agency Official for Privacy (SAOP) will be responsible for its oversight. As required by the Office of Management and Budget (OMB) Memorandum 99-05, "Instructions on complying with President's Memorandum of May 14, 1998," [2] the Assistant Secretary for Management/Chief Financial Officer (ASM/CFO) was assigned the role of SAOP and Chief Privacy Officer (CPO).

For several years, the information privacy function at the Department of the Treasury was split between the Office of Disclosure Services and the Office of the Chief Information Officer (OCIO), both of which are located within the Departmental Offices (DO) at Treasury. Disclosure Services was responsible for handling issues relating to the Privacy Act, in addition to Freedom of Information Act (FOIA) issuances, while OCIO's Information Privacy Program primarily focused on the protection of Personally Identifiable Information (PII).

## B. Re-Organization

### 1. Office of Privacy and Treasury Records

At the direction of the Secretary, through Treasury Order 102-25, "Delegation of Authority Concerning Privacy and Civil Liberties" [3], dated April 30, 2008, and under the leadership of the ASM/CFO, the Office of the Deputy Assistant Secretary for Privacy and Treasury Records (ODASPTR) was created on March 8, 2008. The Office is led by the Deputy Assistant Secretary for Privacy and Treasury Records (DASPTR), who reports directly to the ASM/CFO. The office includes the following functions: privacy, civil liberties, disclosure and Freedom of Information Act services, records management, library services, and the Treasury orders and directives program. The key benefits of the realignment include:

- Consolidation of privacy activities and realignment of management functions;
- Elevation of the privacy functions through the creation of a Deputy Assistant Secretary (DAS) for privacy, who reports directly to the ASM/CFO;
- Consolidation of Treasury-wide business functions for privacy in an effort to promote efficiency; and
- Consistency of policy and execution.

All of the offices within the ODASPTR interact with the Office of Privacy and Civil Liberties (OPCL). The ***Disclosure Services*** staff ensures that first-party FOIA requests are also processed in accordance with Privacy Act laws and that third-party requests contain personal privacy exemptions, as appropriate. The ***Records Management*** staff ensures that records containing PII are handled, retained, stored, and destroyed pursuant to archival guidelines. The ***Library Services*** staff submits legislative history relating to privacy and monitors

1 http://www.treas.gov/regs/td25-04.htm

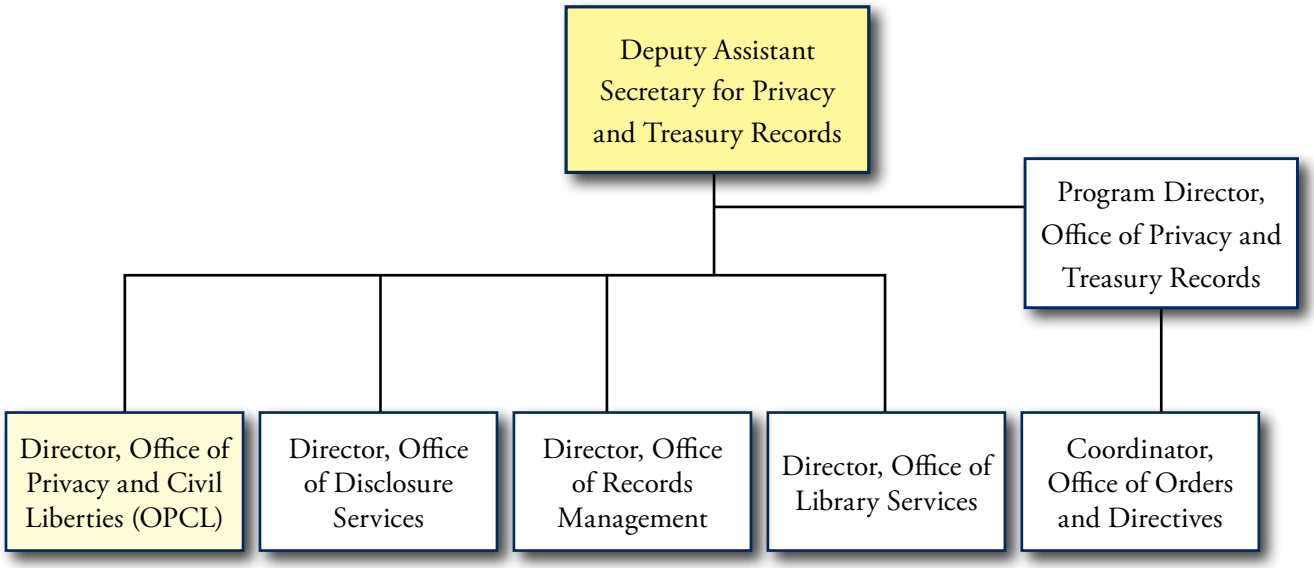
2 http://www.whitehouse.gov/omb/memoranda_m99-05/

3 http://www.treas.gov/regs/to102-25.htm

privacy news for dissemination. The ***Orders and Directives*** staff assists in the establishment and issuances of privacy policies.

### 2. Office of Privacy and Civil Liberties

The OPCL strives to maintain a robust privacy program and is responsible for privacy and civil liberties oversight and compliance throughout the Department. The Director of OPCL reports directly to the DASPTR and works closely with Treasury managers to develop, implement, and monitor agency-wide privacy policies and procedures in compliance with relevant Federal statutes, Executive Orders, OMB memoranda and guidance, other relevant standards, and regulations. The Office also monitors civil liberties activities and works with Departmental Offices and Bureaus to ensure that privacy and civil liberties safeguards are in place. The chart below shows the new organization of the ODASPTR.



### 3. Bureau Responsibilities

As a result of the reorganization, bureau responsibilities for compliance activities were formalized, as was OPCL's responsibility for department-wide reporting oversight (e.g., FISMA and Section 803). Bureau heads are responsible for establishing internal procedures to ensure the effectiveness of their bureau's privacy program and conformity with Treasury-wide privacy requirements. Bureau privacy officers work with their IT representatives to analyze the data being processed in IT systems and determine whether the data contain PII or other protected personal information. This includes performance of Privacy Threshold Analyses (PTAs) and Privacy Impact Assessments (PIAs), described later in this report. In addition, the bureau privacy officers act as liaisons between bureau managers, IT representatives, system owners, and OPCL staff members to ensure that privacy and data protection programs are operating effectively at the bureau level.

## C. Significant Events and Activities

### 1. System of Records Notices

Under the Privacy Act, agencies must assess whether the need to collect and maintain information on individuals exists and they must have plans for collecting, processing, using, storing, and disposing of the information in place. Treasury maintains approximately 210 systems of records, nearly one half of which are maintained by the IRS. Each time such a system is created or altered, OPCL approves the report for OMB about the new system or alteration for publication in the *Federal Register* [4].

Generally, the process of establishing a System of Records Notice (SORN) begins at the bureau, office, or program level, where the collection of information occurs or where the records are maintained. System managers are primary points of contact for receipt of requests for review, access, amendment, and accounting of disclosures. They also notify the departmental or bureau privacy officer when establishing, maintaining, revising, or deleting a system of records. Bureau privacy representatives review their system notices for necessary changes and report this information to OPCL.

The Department also promulgates rules to exempt a system of records from certain provisions of The Privacy Act of 1974, As Amended, (5 U.S.C. 552a), if the records maintained by the Department qualify for one or more of the exemptions under (j)(2) or (k) of the Act. The Department's systems of records for which a Privacy Act exemption has been claimed are identified in 31 CFR 1.36.

### 2. Privacy Impact Assessments

In 2007 and 2008, the Office of Privacy and Civil Liberties took significant steps in strengthening its protections for safeguarding PII. Building on the foundation established through the Privacy Act of 1974 and its amendments, the E-Government Act of 2002 enhanced the Federal Government's responsibilities to safeguard PII and ensure that electronic systems and information technology are secure. Generally, the responsibility for managing IT resources and electronic systems falls within the duties of the OCIO. The Assistant Secretary for Management and Chief Financial Officer (ASM/CFO), as the CPO, oversees the Treasury privacy program and participates in compliance efforts as required under the E-Government Act; this responsibility is further delegated to OPCL. The E-Government Act requires Federal agencies to conduct PIAs for IT systems and collections and to make them publicly available for systems that are not designated as National Security systems.

4 See Table 1. Treasury SORNs, in Appendix D.

Implementing this and other privacy initiatives requires the cooperation and coordination of privacy, IT security, and other program offices that play a significant role in satisfying E-Government requirements. During FY 2008, the Treasury Department completed and published a directive setting out the policy, procedures and responsibilities for conducting and reporting PIAs. TD 25-07, "Privacy Impact Assessment (PIA)", and the corresponding TD Publication 25-07, "PIA Manual"[5], establish the policy for conducting a PIA when developing or procuring IT systems or projects that collect, maintain, or disseminate information that is in an identifiable form from or about members of the public, as well as for conducting a PTA when new IT systems are being planned or existing systems are modified. A PIA is also required when rules allowing the collection of personal information are established or changed. PIAs are an integral part of Federal Government planning for major new technologies or systems, or for modifying existing ones.

### 3. FISMA

The Federal Information Security Management Act of 2002 (FISMA) was enacted as part of the E-Government Act of 2002. FISMA goals include development of a comprehensive framework to protect the government's information, operations, and assets. In response to FISMA, the Department implemented policies and procedures to reduce information security risks. In addition, there is a substantial privacy component included in the FISMA reporting process to ensure that PII is safeguarded appropriately.

Annual reporting of privacy compliance under FISMA involves reporting for sensitive but unclassified systems, IT systems designated as National Security systems, and for certain other Defense Department and Central Intelligence Agency systems of significant importance. In FY 2008, OPCL assumed responsibility for the privacy-related reporting regarding National Security and certain other systems, a task previously handled by OCIO. The Office coordinated FISMA activities with the Departmental Offices and Bureaus that operate designated systems. This data is routinely reported in Section D (Senior Agency Official for Privacy) of the FISMA Report.

In FY 2007, the Quarterly FISMA Reports indicated that 90 percent of all required PIAs had been completed for that year. The completion rate for required SORNs was nearly 80 percent. However, FY 2008 showed significant improvement, with a completion rate of 95 percent for PIAs and a 100 percent completion rate for SORNs.

### 4. Section 803

Title VIII of the Implementing Recommendations of the 9/11 Commission Act of 2007 (Section 803) created new oversight and reporting responsibilities for the Department of the Treasury. The Director of OPCL manages the Section 803 reporting function, and oversees Treasury compliance with applicable statutes and OMB mandates affecting the privacy and civil liberties of U.S. citizens and permanent residents. The reporting of Department-wide privacy complaint and redress activities is another area that directly benefitted from the reorganization, as it places the reporting responsibility under one senior official. In 2009, after conducting a Treasury-wide assessment of privacy complaints, there were no complaints that required a Departmental-level review. There were some reports of Privacy Act appeals; however, Privacy Act denials that resulted in an appeal were mitigated and resolved at the bureau level.

Treasury Directive 25-09, "Privacy and Civil Liberties Activities Pursuant to Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007", P.L. 110-53 (TD 25-09)[6], published on September 3, 2008, formally established the policy of the Department with respect to Section 803. Consequently, heads of bureaus and relevant offices have established internal procedures to ensure accurate and complete reporting to OPCL.

5 http://www.treas.gov/regs/td25-07.htm

6 http://www.treas.gov/regs/td25-09.htm

Treasury is one of seven federal agencies that must report at least quarterly on periodic reviews of Department actions, policies, procedures, guidelines, and related law to ensure that they adequately reflect due consideration of relevant concerns, including privacy protections. The first quarterly report was completed at the end of calendar year 2007. The December 31, 2008, report showed that over 1500 reviews of various policies and procedures had occurred during the last quarter of the year throughout the Department. These included more than 1000 reviews of the use of Social Security Numbers (SSNs) in an effort to eliminate or reduce their use.

## 5. OMB M-07-16

### *a. Routine Use*

OMB Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII)"[7], dated May 22, 2007, directed each federal agency to develop and publish a routine use in order to be able to disclose information regarding a breach to individuals affected by it, as well as to persons and entities that are in a position to assist the agency in preventing or minimizing any harm from a breach. On October 3, 2007, the Department published at 72 FR 56434[8], a routine use for its existing systems of records that permits the Department to share information about a breach with appropriate persons and entities in order to mitigate the harmful effects of the unauthorized disclosure of confidential or private information.

### *b. SSN Reduction*

Under the same OMB memorandum, agencies were directed to eliminate unnecessary use of SSNs. The memorandum set in motion an ongoing Federal government-wide effort. This task also involved exploring alternatives to agency use of SSNs as personal identifiers.

In October 2007, the ASM/CFO in the role of SAOP, called upon departmental offices and bureaus to review their uses of SSNs and develop specific plans to eliminate their use. The instruction from senior management included guidelines for developing and implementing plans. The guidelines requested that bureaus first confirm the SSN Use Survey data that had been compiled earlier in the year at OMB's request, and justify the business need for any continuing use of SSNs as identifiers. The ASM/CFO also asked to receive each bureau's plan for protecting or eliminating SSN information, with milestones, by the beginning of December 2007. Each year, status reports are sent to ODASPTR for review.

During 2008, departmental offices and bureaus implemented their plans to review the uses of SSNs and then further developed plans to eliminate unnecessary uses to the extent possible. The Bureau of Public Debt (BPD), for example, completed its SSN reduction plan ahead of schedule, identifying 17 processes that potentially used SSNs. As a result, BPD either eliminated or replaced the use of SSNs where it was legally possible. Other bureaus continue to assess their uses of SSNs and consider making reductions when there is a sound business case for doing so.

7 http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf

8 www.ustreas.gov/foia/privacy/revised-notice_72fr56434.html

### *c. PII Risk Management Group*

In response to M-07-16, and to meet the requirements of the OMB memorandum dated September 20, 2006, "Recommendations for Identify Theft Related Data Breach Notification",[9] the Department formally established the Personally Identifiable Information Risk Management Group (PIIRMG) on July 7, 2008.

The PIIRMG is an executive response group created to take immediate steps to execute a risk assessment, a risk mitigation plan, and a notification plan in the event of a major privacy breach for the Department or one of its components. The PIIRMG is also chartered to develop policies; evaluate the effectiveness of those policies; evaluate the Department's compliance with applicable privacy laws and regulations; track trends; and identify best practices for continued improvement.

In the event of a major PII breach, the PIIRMG provides senior leadership guidance, and assists the affected departmental office or bureau in mitigating the impact of the breach. The group also provides Department-level concurrence for PII breach notification actions. The PIIRMG's core members are the ASM/CFO, the General Counsel, the DASPTR, the DAS for Information Systems/CIO, and the Deputy Commissioner of Operations Support for the Internal Revenue Service (IRS).[10]

### *d. Training and Awareness*

Training has always been at the forefront of privacy initiatives, to increase Treasury-wide awareness of privacy principles and protections, as well as the appropriate handling of PII. As such, ODASPTR took significant steps to increase the availability of the privacy awareness training. In 2007, privacy training was offered via Treasury's intranet. In response to M-07-16, requiring agencies to annually train employees on privacy and security responsibilities, ODASPTR implemented a mandatory privacy course for Treasury employees entitled, "A Culture of Privacy Awareness." In 2008, ODASPTR enhanced its privacy training courseware and loaded it on the Department's newly-created Treasury Learning Management System (TLMS) platform, which is a web-based platform, available to Treasury offices and bureaus. To go one step further, ODASPTR also implemented role-based privacy training for Treasury managers and IT representatives. The courses entitled, "Implementing Privacy in Treasury Information Systems" and "Privacy and FOIA for Treasury Executives" are also available on TLMS. A course entitled, "Privacy for Treasury Supervisors" is also offered via Treasury's intranet and will be added to the TLMS platform in the near future.

# II. Privacy in the Present (2009)

## A. Privacy Oversight and Compliance

### 1. FISMA

During the past year, the Department of Treasury's privacy program has continued to mature. Progress has been made in the completion of SORNs and PIAs, and the publication of guidance to support various privacy activities across the Department has continued. Although draft procedures were already in use, on June 30,

9 www.whitehouse.gov/omb/assets/omb/memoranda/fy2006/task_force_theft_memo.pdf

10 The Treasury Inspector General, TIGTA, and SIGTARP are advisory members. Other members include the Assistant Secretary (A/S) for Legislative Affairs and the A/S for Public Affairs, DAS for Human Resources, and others.

2009, the Department finalized its publication for PIA guidance, Treasury Directive Publication (TD P) 25-07, "Privacy Impact Assessment (PIA) Manual." In the eighteen months leading up to the official issuance of this guidance, Treasury conducted a series of PIA workshops. In approximately ten presentations of the workshop nearly 250 Treasury employees received formal training in the conduct of successful PIAs.

At the start of FY 2009, ODASPTR began to progress further toward the goal of a 100 percent completion rate for PIAs and SORNs for those systems requiring such assessments and notices. The inventory of sensitive but unclassified (SBU) systems is dynamic. Treasury reported a total of 338 systems that required PIAs and 297 systems that required a SORN. For the first quarter of FY 2009, 99 percent (333) of the Department's systems had current PIAs and 100 percent of the systems requiring SORNs were published in the Federal Register. For the second quarter of FY 2009, there was a slight decrease in the percentage for PIAs and SORNs as the bureau inventories fluctuated. The figures for both declined to 96 and 99 percent, respectively. The Department determined that the decreases were primarily due to the retirement of older systems and changes in the methodology used to count systems. Those bureaus which reported decreases were working to complete the necessary PIAs and SORNs. The percentages were unchanged for the third quarter; but, by the fourth quarter, the trend began to rise, reflecting that 97 percent of the Department's PIAs had been completed. The completion rate for SORNs remained unchanged at 99 percent.

Training is another area that has benefitted from increased OMB guidance and evolving government-wide standards. During the last quarter of FY 2009, the Department reinforced the importance of privacy awareness training Department-wide and achieved a 22% increase in the number of employees who completed the training for FY 2009, as compared to FY 2008.

### 2. Section 803

Similar to FISMA, Treasury made significant strides in broadening its reviews under the Section 803 reporting process. During FY 2009, there were a number of significant achievements in support of this effort.

Early in 2009, The Obama Administration directed a 60-day cyberspace policy review to assess U.S. policies and structures for cyber-security. The review team engaged a cross-section of industry, academia, the civil liberties and privacy communities, state governments, international partners, and the Legislative and Executive Branches to solicit and assess relevant issues including how to improve cyber-security while protecting privacy and civil liberties. Treasury took part in this effort, sending a representative from the ODASPTR to participate in discussions with the review team. The final report was released on May 29, 2009, and included recommendations for 10 near-term actions, including designating a privacy and civil liberties official, and building a cyber-security based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the Nation.

Throughout FY 2009, Departmental Offices and Bureaus were proactive in conducting a variety of reviews; in providing advice and responses to clarify policy positions; and in processing complaints related to privacy and civil liberties. The Department conducted 40 Identity Risk Assessment Reviews, three Persistent Technology Tracking Reviews, 98 A-130 Reviews in support of a variety of programs, and 12 reviews relating to the Paperwork Reduction Act. The Department also issued advice in the form of policy and regulatory guidance to include the issuance of TD 25-06, "The Treasury Data Integrity Board", on January 16, 2009, and TD 25-08, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information", on December 22, 2009.

## B. Intra-agency Coordination

### 1. PII Risk Management Group

As mentioned previously, the PIIRMG is an executive-level, risk-management group designed to assist the affected departmental office or bureau in mitigating the impact of the breach. The group assists by recommending or establishing proactive policies that promote the training of individuals on the protection of PII, procedural safeguards to prevent misuse or unauthorized access to PII, and programmatic accountability in an effort to safeguard against harm to an individual or group as a result of a PII breach. On December 22, 2009, the Department published TD 25-08, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information"[11], which established the Department's policy on handling and protecting PII and reinforced Treasury bureau requirements to develop breach response and notification plans. This Directive also confirms the role of the Department's PIIRMG.

### 2. Treasury Information Privacy Council

To gain Department-level support for privacy initiatives, Treasury established the Information Privacy Council, which is comprised of senior executives who play a critical role in the Department's privacy program. In FY 2009, the Council held its first official meeting and formally adopted its charter. The Council is chaired by the DASPTR, and it meets on a quarterly basis, or as needed. The Council meetings consist of a collaborative forum that allows for the dissemination of information and the discussion of program activities that will be effectuated Treasury-wide. The Council promotes a common vision for privacy objectives, and it is chartered to develop and recommend strategies and actions to guide the Treasury Department's privacy program. Council members provide expert advice to the DASPTR on programmatic, policy, operational, and technological issues that affect information privacy, and they act as stewards within their respective bureaus when privacy initiatives must be accomplished at the highest level.

In FY 2009, the Council members made continual efforts to ensure that bureau employees and contractors received annual privacy awareness training. Council members also played a key role in disseminating draft policies and in gathering comments for final consideration, particularly those policies relating to the protection of PII and breach notification procedures.

### 3. Treasury Information Privacy Committee

The requirements of the Consolidated Appropriations Act of 2005 and the E-Government Act of 2002 highlighted a need for an internal committee to bring privacy and IT professionals together. As a result, the Information Privacy Committee (IPC) was established under the Information Management Sub-Council of the Treasury CIO Council.

The IPC is a collaborative forum, hosted by OPCL, and it is comprised of privacy and IT professionals from each bureau within Treasury. The IPC provides operational level support and assists in the implementation of privacy policies and procedures. The IPC meets bi-monthly or as needed, and has become an excellent source for disseminating information to bureau senior executives, mid-level managers, and their employees and contractors.

The IPC members provide input on newly-formed and existing policies that are developed within and outside of the Department. It has been instrumental in shaping enterprise-wide activities as those activities relate

11 http://www.treas.gov/regs/td25-08.htm

to privacy and data protection. The IPC offers a structured environment for information-sharing among bureau staff members, including those who work in information security, records management, technology management, and the Office of the General Counsel.

The IPC can be credited with quickly gathering and disseminating comments for recently-proposed privacy policies, like TD-25-08, and for reviewing changes to existing policies and procedures like TD P 25-07 (both mentioned earlier). The IPC members were also instrumental in promoting privacy and IT security awareness training throughout their respective bureaus to ensure that the Department complied with the requirements of FISMA. As a result of the diligence of these members, Treasury privacy training efforts have been highly successful.

### 4. Data Integrity Board

The Computer Matching and Privacy Protection Act of 1988 (CMPPA), created new statutory responsibilities for Disclosure Services and the ODASPTR. The CMPPA requires that each Federal agency that acts as either a source or recipient in a matching program establish a Data Integrity Board (DIB) to oversee the agency's participation. The Act requires that a Board consist of senior agency officials designated by the agency head. The Treasury DIB is made up of six permanent representatives and three rotational representatives. Treasury's DIB evaluates the proposed match and approves the terms of the matching agreement before any component of Treasury participates in a matching program. Matching programs provide a direct benefit to members of the public by assisting in the elimination of errors and omissions of data, and in monitoring waste, fraud, and abuse.

Although the OCIO provides the day-to-day operational support for the DIB, a Departmental privacy officer (presently in OPCL) serves as a permanent member, acts as the secretary to the Board, and maintains the minutes of Board meetings. The Departmental privacy officer is also responsible for policy guidance and direction on privacy protection matters with respect to computer matching and implementing sections of the Computer Matching Act concerning the protection of the privacy rights of individuals. The Departmental privacy officer coordinates, reviews, revises, and submits notices for computer matches covered under the provisions of the CMPPA to Congress and the Federal Register on behalf of Treasury[12].

## C. Interagency Collaboration

### 1. CIO Council/ Privacy Committee

In 1996, the Chief Information Officers (CIO) Council was established by Executive Order, and enacted by Congress in the E-Government Act of 2002. As a result, CIOs and Deputy CIOs from more than two dozen Federal executive departments and agencies participate in this interagency forum for improving practices in the design, modernization, use, sharing, and performance of Federal Government agency information resources. The Deputy Director for Management for OMB chairs the Council, and the Vice Chair is elected by the members.

There are five committees, including a privacy committee, that form the operational underpinnings of the CIO Council. FY 2009 marks the first full year that the privacy committee has been in operation, and the DASPTR serves as the Treasury representative. On an on-going basis, employees of the Department continue to be active in these interagency privacy forums. Treasury employees currently serve on the Best Practices,

12 See Table 2. Treasury Computer Matching Agreements, in Appendix D.

Web 2.0, Development and Education, and International Subcommittees of the Federal CIO Council's Privacy Committee.

The Best Practices subcommittee is working with member agencies to assist them in establishing a robust privacy program. This subcommittee has been reviewing risk management tools and techniques, and it has recently submitted a Federal Enterprise Architecture Security Privacy Profile for OMB review. The Web 2.0 subcommittee has been instrumental in navigating its member agencies through the technological advances of social media. This subcommittee has played a major role in proposing revisions to the federal guidance pertaining to persistent cookies, and in revising the model terms of service agreements between government agencies and internet companies, which are awaiting OMB review. The Development and Education subcommittee not only played a role in training CPOs and SAOPs in their roles as leading privacy officials, the subcommittee was also instrumental in training privacy and IT professionals from across the Federal Government in the 2009 Federal Privacy Summit. The PTR Office co-chaired the planning effort for that summit. Lastly, the International subcommittee is instrumental in keeping members of the intelligence community, like the Department of the Treasury, abreast of changes to international laws as they relate to privacy. The subcommittee also assists Departments in handling privacy issues involving foreign nationals.

### 2. Information Sharing Environment

Following the attacks of September 11, 2001, the President and Congress acted to foster greater sharing of terrorist information within the government and between government and the private sector.[13] In December 2004, Congress followed with the Intelligence Reform and Terrorism Prevention Act (IRTPA), which established the Information Sharing Council (ISC) as part of an overall effort to promote an information sharing environment (ISE). The President ordered that Treasury, among other agencies, be represented on the Council.

Throughout this time, Treasury contributed to the ISE's efforts and, in particular, facilitated the development of the ISE Suspicious Activity Report Functional Standard, and the ISE Architecture framework. The ASM/CFO is the Department's Senior Agency Official for Information Sharing. The CIO is the lead representative on the ISC, and the Associate CIO for E-Government is the alternate. The OCIO closely coordinates with those departmental offices and bureaus that have an intelligence element. The OCIO also routinely communicates with OPCL, the Records Office, and the Office of General Counsel.

In September 2007, in accordance with Section 1016 of IRPTA, the ISE Program Manager issued The Privacy and Civil Liberties Implementation Guide for the ISE, and the first report to Congress on the ISE was also released. Additionally, the ISE Privacy Guidelines Committee instructed its member agencies to draft a privacy policy relating to information sharing within the intelligence community. In 2009, OPCL completed its initial draft of TD 25-10, "Information Sharing Environment Privacy Policy." This draft directive promotes a duty to share information and give the highest priority to the interchange of terrorism, homeland security, and law enforcement information. Presently, member agencies are sharing their ISE privacy policy

13 EO 13356, Sharing of Terrorism Information to Protect Americans, August 7, 2004. (http://nodis3.gsfc.nasa.gov/displayEO.cfm?id=EO_13356_) The ISC advises the President and the Program Manager on the development of ISE policies, procedures, guidelines, and standards, and ensures proper coordination among federal agencies participating in the ISE. The President designated the Program Manager and directed that the Office of the PM-ISE be located in the Office of the Director of National Intelligence. On October 25, 2005, the President issued Executive Order 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans, (http://edocket.access.gpo.gov/2005/pdf/05-21571.pdf), which superseded Order 13356, and restructured the Information Sharing Council (ISC), bringing it into alignment with the requirements of IRTPA. The EO specified that the Treasury Department, among other Federal departments and agencies, would be represented on the Information Sharing Council.

drafts in a collaborative zone so that policy details are openly discussed to assist agencies in their efforts to finalize their ISE policies.

## D. Other Events and Activities

### 1. Office of Financial Stability

At the end of 2008, a new financial and economic crisis of global proportions unseen by most Americans erupted. This led to the creation of the Office of Financial Stability (OFS) and the Troubled Asset Relief Program (TARP), which were designed to assist distressed financial institutions. All components of ODASPTR were called upon to assist the new but rapidly expanding part of Treasury. The privacy office played a major role in assisting OFS as it stood up its systems to assist banks, as well as members of the public.

To the extent that the TARP collects, uses, discloses, or maintains personal information from banks about members of the public, the program turned to ODASPTR for direction on how to protect the privacy of the subject individuals and how to secure the data and the systems that hold or transmit personal data.

### 2. TARP

New programs instituted by TARP have required the identification of Privacy Act systems of records, and publication of required SORNs. ODASPTR has supported OFS with both efforts. One such system of records, entitled Treasury/DO .218 - Home Affordable Modification Program, was necessary for the administration of the Home Affordable Modification Program (HAMP), which allows eligible homeowners who are current but having difficulty making their mortgage payments to modify their loan with more affordable monthly payments. An additional SORN, entitled Treasury/DO .219 TARP Standards for Compensation and Corporate Governance--Executive Compensation Information System, was also recently published in the Federal Register.

### 3. SIGTARP

The Office of the Special Inspector General for the Troubled Asset Relief Program (SIGTARP) was created as an independent agency within Treasury responsible for conducting, supervising, and coordinating audits and investigations of any actions taken under the Emergency Economic Stability Act of 2008, as amended by the Special Inspector General for the Troubled Asset Relief Program Act of 2009. OPCL has provided SIGTARP with significant support in the establishment of its systems of records that contain information about individuals. In accordance with the Privacy Act and Departmental regulations, SIGTARP published several SORNs on January 14, 2010.

In addition, OPCL assisted SIGTARP in its publication of a proposed rule amending 31 CFR 1.36, Treasury's Privacy Act regulations, by claiming exemptions under the Privacy Act pursuant to 5 U.S.C. 552a(j)(2) and (k)(2) for its SORNs. SIGTARP activities qualify as a "principal function" criminal law enforcement component and meet the criteria for claiming an exemption pursuant to Section (j) (2) of the Privacy Act, and (k)(2) "investigatory material compiled for law enforcement purposes, other than material within the scope of subsection (j) (2)."

### 4. IRS Office of Privacy, Information Protection & Data Security

As part of the IRS Privacy Information Protection and Data Security (PIPDS) organization, a specialized unit, the On-line Fraud Prevention and Detection (OFDP) unit, was established to detect and prevent online fraud designed to steal taxpayers' identity and other PII information. Typically, the fraudsters send out phishing emails, purported to be from the IRS, requesting PII or to implant malicious viruses to steal taxpayers' financial account data and/or passwords. In the three years since OFDP was established, IRS has been successful in shutting down close to 9,000 phishing web sites.

It is expected that IRS will remain one of the top targeted phishing brands. In 2009, industry source Phishtank consistently ranked IRS in the top 10 targeted phishing brands, and 50% of the time ranked it as the number two target (second only to Paypal), underscoring the broad efforts of phishers and highlighting the need for IRS's continued vigilance.

# III. Privacy in the Future

## A. Open Government, Web 2.0, and the Clouds

On January 21, 2009, President Obama signed a memorandum for Transparency and Open Government, which prompted Federal agencies like Treasury to explore new ways to disseminate information to members of the public.[14] The increasing use of social media to reach all generations and to solicit public feedback has spurred Treasury to harness new technologies to make information readily available to the public.

Treasury offices and bureaus have begun to consider and use some of the social networking tools, such as Facebook, Twitter, Flickr, and others. The term "Web 2.0" is commonly associated with web applications that facilitate interactive collaboration, interoperability, information sharing, and user-centered design on the World Wide Web.[15] Examples of Web 2.0 include, but are not limited to, web applications, web-based communities, social-networking sites, video-sharing sites, hosted services, wikis, and blogs.

Another new facet of technology service delivery is the advancement of cloud computing. **Cloud computing** is an internet-based concept of computing, storage, and bandwidth service provisioning that relieves users from needing expertise in, or control over, the technology infrastructure, since it is provisioned "in the clouds."[16] Despite attractive pricing and convenience, there are risks involved with using cloud computing because agencies typically do not own the physical infrastructure and data is housed outside of the agency infrastructure, which decreases their ability to protect sensitive data. As with social media concerns, the privacy office will explore new issues surrounding this type of technology and seek to ensure that Treasury bureaus and offices institute appropriate policies to safeguard PII and other privacy-related data.

Regardless of what drives the Department's decision to utilize advanced technologies, the fact remains that there are privacy and data protection risks involved. Although the Department welcomes new technology, it will remain diligent in managing all risks to the sensitive data and PII that the Department handles. Therefore,

14 http://www.whitehouse.gov/the_press_office/TransparencyandOpenGovernment/

15 Sharma, P. (2008, November 28). *Core Characteristics of Web 2.0 Services*. Retrieved from: www.techpluto.com/web-20-services

16 *Cloud Computing*. Retrieved from: http://en.wikipedia.org/wiki/Cloud_computing

in addition to monitoring oversight and compliance with privacy laws and other mandates, ODASPTR will seek to ensure that policies are created to focus on user behavior and to reinforce appropriate procedures when accessing, collecting, and disseminating personal information. The Department's efforts to mitigate risks in these and other areas of new technology will be discussed in its next annual report for privacy.

# IV. APPENDICES

## Appendix A. Acronyms

| | |
|---|---|
| ASM/CFO | Assistant Secretary for Management and Chief Financial Officer |
| CIO | Chief Information Officer |
| CMPPA | Computer Matching and Privacy Protection Act of 1998 |
| CPCLO | Chief Privacy and Civil Liberties Officer |
| CPO | Chief Privacy Officer |
| DAS | Deputy Assistant Secretary |
| FISMA | Federal Information Security Management Act of 2002 |
| FOIA | Freedom of Information Act |
| GAO | General Accountability Office |
| IG | Inspector General |
| IIF | Information in Identifiable Form |
| IPC | Information Privacy Committee |
| IRS | Internal Revenue Service |
| IT | Information Technology |
| NIST | National Institute of Standards and Technology |
| OCIO | Office of the Chief Information Officer |
| OCPCLO | Office of the Chief Privacy and Civil Liberties Officer |
| ODASPTR | Office of the Deputy Assistant Secretary for Privacy and Treasury Records |
| OFS | Office of Financial Stability |
| OIG | Office of the Inspector General |
| OMB | Office of Management and Budget |
| OPCL | Office of Privacy and Civil Liberties |
| OPTR | Office of Privacy and Treasury Records |
| PCLOB | Privacy and Civil Liberties Oversight Board |
| PIA | Privacy Impact Assessment |
| PII | Personally Identifiable Information |
| PIIRMB | PII Risk Management Group |
| PTA | Privacy Threshold Analysis |
| SAOP | Senior Agency Officer for Privacy |
| SIGTARP | Special Inspector General for TARP |
| SOR | System of Records |
| SORN | System of Records Notices |
| TARP | Troubled Asset Relief Program |
| TIGTA | Treasury Inspector General for Tax Administration |
| US-CERT | U.S. Computer Emergency Readiness Team |

## Appendix B. List of Key Laws and Regulations Applicable to Treasury Department Privacy Activities

- **31 CFR Part 1, Treasury privacy regulations**
- **Clinger-Cohen Act of 1996**, formerly Section 5131 of the Information Technology Management Reform Act of 1996, P.L. No. 104-113, (requires government information technology shops to be operated exactly as an efficient and profitable business would be operated. Acquisition, planning and management of technology must be treated as a "capital investment." The statute affects all consumers of hardware and software in the Department, and is performed in conjunction with the CIO's office)
- **Consolidated Appropriations Act of 2005**, Division H, Title II, Section 522, (requiring specific agencies to submit an annual report to Congress on Department activities that affect privacy)
- **E-Government Act of 2002**, P.L. 107-347, section 208, (requires an annual report to Congress requiring agencies to describe efforts to accomplishing E-Gov initiatives, to include capital planning, and include an executive summary highlighting significant issues); however, E-Gov encompasses numerous requirements/initiatives
- **Executive Order 13388**, Further Strengthening the Sharing of Terrorism Information to Protect Americans, (establishes the requirement ISE communities to create IT and Privacy Guidelines for sharing terrorist information)
- **Federal Information Security Management Act of 2002**, P.L. No. 107-347, (requires all federal agencies to develop, document, and implement agency-wide information security programs for the information and information systems that support the operations and the assets of the agency, including those provided or managed by another agency, contractor, or other source)
- **Intelligence Reform and Terrorism Prevention Act of 2004** (IRTPA), P.L. 108-458, Section 1016(d) (created to reform the intelligence community and the intelligence and intelligence-related activities of the U.S. Government, and for other purposes)
- **The Freedom of Information Act, as amended, Title 5, U.S.C. § 552, provides for the disclosure of information maintained by Federal agencies to the public while allowing limited protections for privacy.**
- **National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 199**, Standards for Security Categorization of Federal Information and Information Systems (addresses one of the requirements specified in the FISMA)
- **National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 200**, Minimum Security Requirements for Federal Information and Information Systems, (this is the second standard that was specified by the FISMA and is an integral part of the risk management framework. This is performed in conjunction with the CIO's office.)
- **National Institute of Standards and Technology (NIST) Standards Publication (SP) 800-53** (soon to be FIPS 200) (in conjunction w/ FISMA requirements, SP 800-53 requires Federal organizations to implement controls by streamlining their business processes to assure business continuity, improve operational efficiency and maximize security for the IT infrastructures of those organizations)
- **National Institute of Standards and Technology (NIST) Standards Publication (SP) 800-122 (Draft)**, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

- **OMB Circular A-130, Management of Federal Information Resources, (**provides instructions to Federal agencies on how to comply with the fair information practices and security requirements for operating automated information systems.)
- **OMB M-99-05** provides instructions for complying with President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records"
- **OMB M-05-08**, Designation of Senior Agency Officials for Privacy
- **OMB M-06-15**, Safeguarding Personally Identifiable Information
- **OMB M-06-16**, Protection of Sensitive Agency Information
- **OMB M-06-19**, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments
- **OMB M-06-20**: FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management. New FISMA Privacy Reporting Requirements for FY 2008
- **OMB Memo Sept. 20, 2006**, Recommendations for Identity Theft Related Data Breach Notification
- **OMB M-07-16**, Safeguarding Against and Responding to the Breach of Personally Identifiable Information
- **OMB M-08-21**: FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
- **Privacy Act of 1974** (PA), (provides overall guidance to Federal entities re privacy protections for U.S. and naturalized citizens); PA Systems of Records Notices are routinely needed (to notify the public about what records the Federal government retains/retrieves and its purpose for collection)
- **Section 803 of the Implementing the Recommendations of the 9/11 Commission Act of 2007**, P.L. No. 110-53
- **Treasury Order 102-25,** Delegation of Authority Concerning Privacy and Civil Liberties
- **Treasury Directive 12-54**, Approval of Privacy Act Documents; authority delegation
- **Treasury Directive 25-04 (Draft)**, Privacy Act of 1974, (reflects OPTR as a new organization, provides clearer guidance, and address GAO redress concerns)
- **Treasury Directive 25-07**, Privacy Impact Assessment (PIA), (provides guidance to Treasury Bureaus on determination and completion of PIAs)
- **Treasury Directive (Draft) 25-08**, Personally Identifiable Information (PII) Breach Response and Notification
- **Treasury Directive 25-09**, Privacy and Civil Liberties Activities Pursuant to Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53**.**

## Appendix C. List of Treasury Department Bureaus and Offices

Bureau of Engraving and Printing (BEP)

Bureau of Public Debt (BPD)

Community Development Financial Institutions Fund (CDFI)

Departmental Offices (DO, also known as Headquarters)

Financial Crimes Enforcement Network (FinCEN)

Financial Management Service (FMS)

Internal Revenue Service (IRS)

United States Mint (Mint)

Office of the Comptroller of the Currency (OCC)

Office of the Inspector General (OIG)

Office of Thrift Supervision (OTS)

Special Inspector General for TARP (SIGTARP)

The Alcohol and Tobacco Tax and Trade Bureau (TTB)

Treasury Inspector General for Tax Administration (TIGTA)

# Appendix D. Tables

## Table 1. Treasury SORNs 2007-2009

| SORN | Publication Date | Federal Register |
|---|---|---|
| Revised U.S. Mint SORN | January 29, 2007 | 72 FR 4325 |
| Revised FMS SORN | March 2, 2007 | 72 FR 9611 |
| Alterations to 6 OTS SORNS | April 18, 2007 | 72 FR 19580 |
| Treasury-wide routine use | October 3, 2007 | 72 FR 56434 |
| Internal Revenue Service | March 12, 2008 | 73 FR 13284 |
| Comptroller of the Currency | July 18, 2008 | 73 FR 41402 |
| Financial Crimes Enforcement Network | July 21, 2008 | 73 FR 42405 |
| United States Mint | July 22, 2008 | 73 FR 42662 |
| Bureau of the Public Debt | July 23, 2008 | 73 FR 42904 |
| Alcohol and Tobacco Tax and Trade Bureau | September 2, 2008 | 73 FR 51344 |
| Financial Management Service | May 15, 2009 | 74 FR 23006 |
| DO, Office of DC Pensions | June 22, 2009 | 74 FR 29532 |
| Office of Thrift Supervision | June 29, 2009 | 74 FR 31090 |
| Bureau of Engraving and Printing | June 29, 2009 | 74 FR 31090 |
| Bureau of Public Debt | July 17, 2009 | 74 FR 34867 |
| Office of Financial Stability | July 24, 2009 | 74 FR 36823 |
| DO | October 28, 2009 | 74 FR 55621 |
| Bureau of Engraving and Printing | December 30, 2009 | 74 FR 69190 |

## Table 2. Treasury Computer Matching Agreements - 2009

| Bureau/Office | Matching Agreement |
|---|---|
| Internal Revenue Service | Disclosure of Information to Federal, State and Local Agencies (DIFSLA) |
| | Medicare Secondary Payer Program |
| | Medicare Prescription Drug Subsidy Program |
| | Medicare Part B Premium Reduction |
| | Telecommunications Asset Tool (TAT) |
| Bureau of the Public Debt | Eligibility under the SSI, and Medicare Prescription Drug Program |
| Treasury Inspector General for Tax Administration | Detecting unauthorized browsing and deterring fraud, waste, and abuse in IRS programs and operations |
| Financial Management Service | Treasury Offset Program (TOP) |