Department of the Treasury

2010 Annual Report for Privacy

(October 1, 2009 – September 30, 2010)

[An electronic copy of this report is available at
http://www.treasury.gov/FOIA/Pages/privacy_index.aspx.]

Message from the Chief Privacy Officer (CPO)

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

As the Assistant Secretary for Management (ASM), Treasury's designated Chief Privacy Officer (CPO), Senior Agency Official for Privacy (SAOP), and Chief Privacy and Civil Liberties Officer (CP&CLO), I am pleased to present the Department of the Treasury's 2010 Annual Report for Privacy. This is the second installment of the Department's Annual Report for Privacy since the Treasury's privacy program underwent structural change. This report covers the period from October 1, 2009 through September 30, 2010. The report contains three (3) primary sections that provide an overview of the Treasury's privacy program, the Treasury's 2010 major activities and accomplishments dealing with privacy, and the 2011 outlook for privacy in the Department of the Treasury.

Section I, entitled "Overview," provides a short description of the privacy policy that outlines both the rules and regulations that the Department has to implement and enforce, and the reporting requirements for the Department when dealing with privacy related topics. This section also provides a description of the duties and responsibilities of the Office of Privacy and Civil Liberties (OPCL). Finally, this section outlines the goals and performance measures for OPCL to ensure the Department is able to measure and report on ongoing privacy initiatives and plans of actions.

Section II, entitled "Privacy 2010 at a Glance," outlines the Treasury's major activities and accomplishments dealing with privacy. One of the major accomplishments this section covers is the assessment of the Personally Identifiable Information (PII) holdings across the Department. In FY 2010, I instructed OPCL to execute a survey to assess and identify electronic and paper systems containing PII. The assessment helped the Department to inventory the amount of automated and paper systems in use by its employees and contractors. The assessment also brought to light differing views of what constitutes PII and the handling of PII, which led to OPCL initiating an update to the annual privacy training that all Treasury employees and contractors are required to take. Additional privacy awareness and training initiatives, which OPCL coordinated or participated in, are also presented in this section.

Section II also presents the yearly metrics that the Department is required to report on such as Federal Information Security Management Act (FISMA) of 2002 reporting and Section 803 reporting. Along with these metrics, Section II highlights the interagency and intra-agency coordination activities that OPCL takes part in to keep abreast of any new policy or guidance dealing with privacy. This section also provides a list of Treasury Orders and Directives that OPCL developed or took part in their development.

The final section III, entitled "Privacy 2011 Outlook," provides information on the 2011 privacy initiatives in the Department. In response to the differing opinions of what constitutes PII, OPCL will update the annual privacy training to address the identified areas for improvements. This section also covers the update to the PII assessment that will be done on a yearly basis. In 2011, Treasury offices will be able to complete the assessment electronically via the online PII holdings database. The Department will continue to report on the required privacy metrics as well as taking part in different intra-agency and interagency activities in order to disseminate new policy and guidance to the Departmental Offices (DO) and Bureaus.

Executive Summary

The mission of the Office of the Deputy Assistant Secretary for Privacy, Transparency, and Records (ODASPTR) is to serve the public and the Federal government community by setting the standard for protecting, enabling access, retaining, preserving, and disclosing Treasury's information. After two (2) full years of operation as ODASPTR, Treasury is making continued progress to strengthen the protection of citizens' information.

The mission of the Office of Privacy and Civil Liberties (OPCL) is to provide the public with assurances that the information the Department of Treasury collects is being maintained within all mandated requirements. OPCL accomplishes its mission by focusing on the following core activities:

- Provide oversight to the Departmental Offices (DO) and Bureaus to ensure compliance with federal privacy and disclosure laws;
- Propose, develop, and implement laws, regulations, policies, procedures, and guidelines regarding privacy;
- Provide leadership and guidance to promote a culture of privacy across the Department that adheres to privacy standards through workshops, and training opportunities;
- Advance privacy protections throughout the federal government through active participation in interagency forums, and
- Ensure transparency to the public through published materials, reports, formal notices, public workshops, and meetings.

This annual report provides a more detailed explanation of the activities and initiatives that OPCL has either implemented or been a part of to ensure that a culture of privacy has been embedded throughout the Department according to Federal laws and guidelines. During fiscal year 2010 (October 1, 2009 – September 30, 2010), OPCL was able to accomplish and build upon the initiatives from last year's report while demonstrating its continued leadership within and outside of the Department as an essential member of the Federal and international privacy community.

As a part of its responsibility to provide oversight and compliance, OPCL has:

- Completed an assessment of the Department's paper and automated holdings of Personally Identifiable Information (PII). The assessment documented the existence of 422 automated systems containing PII holdings across the Department. The assessment also confirmed the existence of 153 paper systems containing PII across the Department;
- Approved and published seven (7) System of Records Notices (SORNs), of which two (2) were compilations to cover Treasury wide and DO SORNs;
- Provided timely submissions of the FISMA report to the Office of Management and budget (OMB) on behalf of the Department;

- Provided timely submissions of the Section 803 metrics to Congress on behalf of the Department
- Enhanced the Department's annual privacy training by implementing a pre-test for employees to assess their knowledge of privacy principles;
- Provided privacy training opportunities for Treasury and other Federal agencies employees' by sponsoring a privacy week that consisted of workshops, speakers, panel discussions, and the private sector; and
- Hosted a privacy breach-training course that was attended by 85 individuals representing over 30 federal agencies.

As far as providing coordination within the Department, between the DOs and Bureaus, and with outside agencies, OPCL has:

- Secured 150 corporate memberships with the International Association of Privacy Professionals (IAPP) for Department of the Treasury employees';
- Supported Treasury's Information Privacy Council by continuing to host the Information Privacy Committee (IPC). The IPC is a collaborative forum that assists with implementing privacy policies and procedures across the Department;
- Supported the Chief Information Officer (CIO) Council's Privacy Committee by serving on all of the Council's subcommittees;

OPCL has also:

- Processed four (4) directives, of which three (3) of them are Treasury-wide directives; and
- Provided support to the new financial reform entities, e.g. Consumer Finance Protection Bureau (CFPB), Office of Financial Research (OFR), Federal Insurance Office (FIO), Financial Stability Oversight Committee (FSOC), and Small Business Lending Fund (SBLF).

As we move into the next era, with the increasing pace of technology producing new areas of concerns when it comes to privacy, OPCL is poised to be a proactive member of the privacy community to ensure that Department as well as the Federal government keeps pace with the ever-changing issues resulting from a "borderless" cyberspace society.

Table of Contents

Message from the Chief Privacy Officer (CPO) ..... **i**

Executive Summary ..... **iii**

I. Overview **1**

A. Privacy Policy 1
1. Privacy Act 1974 1
2. Systems of Records Notices (SORNs) 1
3. Privacy Impact Assessments (PIAs) 1
4. Federal Information Security Management Act of 2002 (FISMA) 2
5. Section 803 2
B. Organizational Structure 2
1. Office of Privacy and Civil Liberties 2
C. Goals and Performance Measures 3
1. Goals 3
2. Performance Measures 3

II. Privacy 2010 at a Glance **4**

A. Privacy Oversight and Compliance 4
1. Annual PII Assessment 4
a. Automated PII Holdings 5
b. Paper PII Holdings 7
2. SORNs Published 8
3. FISMA Reporting 9
4. Section 803 Reporting 10
5. Privacy Awareness and Training 12
a. Mandatory Privacy Awareness Course 12
b. Privacy Week 12
c. PII Breach Training 13
B. Intra-agency Coordination 13
1. International Association of Privacy Professionals (IAPP) 13
2. Treasury Information Privacy Council and Committee 13
a. Information Privacy Council 13
b. Information Privacy Committee 14
3. Treasury Computer Security Information Response Center (TCSIRC) Reporting 15
4. PII Risk Management Group (PIIRMG) 15
C. Inter-agency Coordination 15
D. Orders and Directives 16
1. Treasury Directive (TD) 25-04 16

2. Treasury Directive (TD) 25-08 16
3. Departmental Offices (DO) Directive 305 17
E. Other Significant Events 17

III. Privacy 2011 Outlook 17

A. Privacy Oversight and Compliance 17
B. Intra-Agency and Inter-Agency Coordination 18
C. Privacy Awareness and Training 18

IV. Appendices A-1

Appendix A List of Acronyms A-1
Appendix B List of Key Laws and Regulations Applicable to Treasury Department Privacy Activities B-1
Appendix C List of Department of Treasury Bureaus and Offices C-1
Appendix D Reference Tables D-1
Appendix E List of Figures E-1
Appendix F List of Tables F-1

I. Overview

A. Privacy Policy

1. Privacy Act 1974

The Privacy Act of 1974 protects certain records collected by the Federal Government on members of the public from unauthorized disclosure and provides access rights to the covered individual. The records are stored in what is called a System of Records. The specific types of records are records that are retrieved from the system by some type of personal identifier (e.g., name, social security number, etc.). Regulations for how Treasury employees maintain, collect, use or disseminate records pertaining to individuals were published in 31 CFR Part 1, Subpart C, on October 2, 1975. These regulations provide procedures by which an individual may request notification of whether the Department of the Treasury maintains or has disclosed a record pertaining to them or may seek access to such records maintained in any nonexempt system of records, request correction of such records, appeal any initial adverse determination of any request for amendment, or may seek an accounting of disclosures of such records.

2. Systems of Records Notices (SORNs)

Under the Privacy Act, agencies must assess whether they need to collect and maintain information on individuals, and they must have plans for collecting, processing, using, storing, and disposing of the information in place. The Treasury Department maintains approximately 216 systems of records, nearly one-half of which are maintained by the IRS. Each time such a system is created or altered, the Office of the Deputy Assistant Secretary for Privacy, Transparency, and Records (ODASPTR) approves the notice and reports to Office of Management and Budget (OMB) and Congress prior to its publication in the *Federal Register*.

3. Privacy Impact Assessments (PIAs)

The E-Government Act requires Federal agencies to conduct Privacy Impact Assessments (PIAs) for IT systems and collections and to make them publicly available for systems that are not designated as National Security Systems.

The Department completed and published a directive, Treasury Directive (TD) 25-07, “Privacy Impact Assessment (PIA)," setting out the policy, procedures and responsibilities for conducting and reporting PIAs. Corresponding guidelines provided in the TD-P 25-07 "PIA Manual,” set out 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 Privacy Threshold Analysis (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. Treasury PIAs can be located at http://intranet.treas.gov/rim/privacy/default.asp.

4. Federal Information Security Management Act of 2002 (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 Treasury 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 Personally Identifiable Information (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 other Defense Department and Central Intelligence Agency systems of significant importance. In FY 2008, the Office of Privacy and Civil Liberties (OPCL) under ODASPTR, assumed responsibility for the privacy-related reporting regarding National Security and certain other systems for Treasury. The Office coordinates FISMA activities with the Departmental Offices and Bureaus that operate designated systems. This data is routine ly reported in Section D (Senior Agency Official for Privacy) of the FISMA Report.

5. 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. Treasury Directive (TD) 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, 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 ODASPTR.

The Director of OPCL manages the Section 803 reporting function, while it oversees Treasury compliance with applicable statutes and OMB mandates affecting the privacy and civil liberties of U.S. citizens and permanent residents. The quarterly reporting of Department-wide privacy complaint and redress activities to Congress, the Secretary of the Treasury, and the Privacy and Civil Liberties Oversight Board, are some of the reporting responsibilities designated to the ASM/CFO.

B. Organizational Structure

1. Office of Privacy and Civil Liberties

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 Deputy Assistant Secretary for Privacy, Transparency, and Records (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.

C. Goals and Performance Measures

1. Goals

OPCL supports OPTR's goal, to "improve the office of Privacy, Transparency, and Records' performance through collaborative strategies based on information sharing and open communication with Treasury and other agency partners." To improve privacy across the Department, OPCL plans to do the following:

- Increase the privacy awareness of Treasury employees through initiatives that reinforce privacy principles in everyday activities for safeguarding the public's PII throughout the Department
- Provide oversight to the Department on privacy related issues and compliance to enhance the Department's information protection practices

2. Performance Measures

Table 1 displays the performance measures that will be used to provide information as to the effectiveness of OPCL in achieving its goals.

Table 1 OPCL's Compliance Performance Measures

Performance Measure	Definition	Threshold Value	Objective Value
Online Training Completion Percentage (TC %)	Percent of the number of Treasury employees/contractors that have completed the online privacy training course (Number of Treasury employees/contractors completed training divided by the total number of Treasury employees/contractors required to take training)	95%	100%
Percent (%) SORNs documented	Percent of systems requiring SORNs that have one documented	95%	100%
Percent (%) PIAs published	Percent of systems requiring a PIA that have one published in the *Federal Register*	95%	100%
Percent (%) reduction of PII Holdings	Percent reduction in the total number of Treasury-wide systems across the department that contain PII	Currently being baselined	Currently being baselined
Percent (%) reduction of PII data breaches	Percent reduction in the total number of Treasury-wide data breaches containing PII	Currently being baselined	Currently being baselined

II. Privacy 2010 at a Glance

A. Privacy Oversight and Compliance

1. Annual PII Assessment

Section 522 of the Consolidated Appropriations Act of 2005, paragraph (c) entitled, "Recording" states that the agency Chief Privacy Officer (CPO) is mandated to… "prepare a written report of its use of information in an identifiable form, along with its privacy and data protection policies and procedures and record it with the Inspector General of the agency to serve as a benchmark for the agency."

During FY 2010, the Senior Agency Official for Privacy (SAOP) required all Bureau and Departmental Offices (DO) heads to complete an assessment of their automated and paper systems that contain PII.

For this assessment, the DO and Bureaus were directed to use OMB's definition of PII. OMB defines PII as "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

With all the data that was collected from the DO and Bureaus, it was evident the data would need to be stored electronically in order to for it to be analyzed efficiently. OPCL worked with the Office of the Chief Information Officer (OCIO) to develop a database that houses the Treasury-wide PII holdings inventory. The database will improve OPCL's oversight capabilities by providing up-to-date reports on Treasury PII holdings as needed, and in the event of special cases (for example, a data breach).

A point of clarification that should be noted is the fact that this inventory of systems, per the PII assessment, was much broader than the ones that constitute systems covered by FISMA. FISMA systems correlate with major investment systems; however, this particular inventory included many standalone minor systems, paper systems, and record-keeping processes. Thus, in this case, the data frequently reported under FISMA for SORNs and PIAs is likely different from the data presented from the PII assessment. **Figure 1** is an illustration that depicts the relationship between the systems inventoried per the PII assessment and the systems inventoried to satisfy the annual FISMA reporting requirements. The blue shaded circle represents the systems inventoried via the PII holding assessment. The green shaded circle represents the set of systems reported via the FISMA annual report. Notice that some of the systems reported in the FISMA report are not included in the systems with PII. The final purple shaded circle represents the subset of FISMA systems that are required to have a documented SORN and PIA.

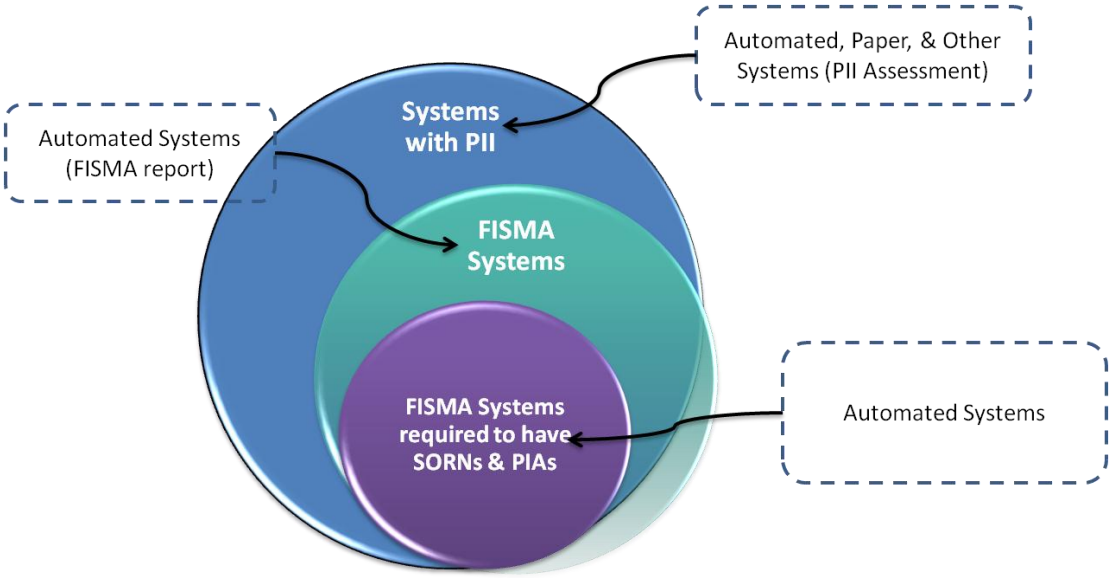

Figure 1 Treasury PII Systems Relationships

a. Automated PII Holdings

A summary of the assessment performed to determine the inventory of the PII holdings across the Department are displayed in **Figure 2** and **Figure 5** for the automated and paper systems, respectively.

Figure 2 displays that 422 automated systems containing PII holdings exist across the Department. Both the Internal Revenue Service (IRS) and the Bureau of Public Debt (BPD) combined for more than 60 percent of the amount of automated systems with PII holdings.

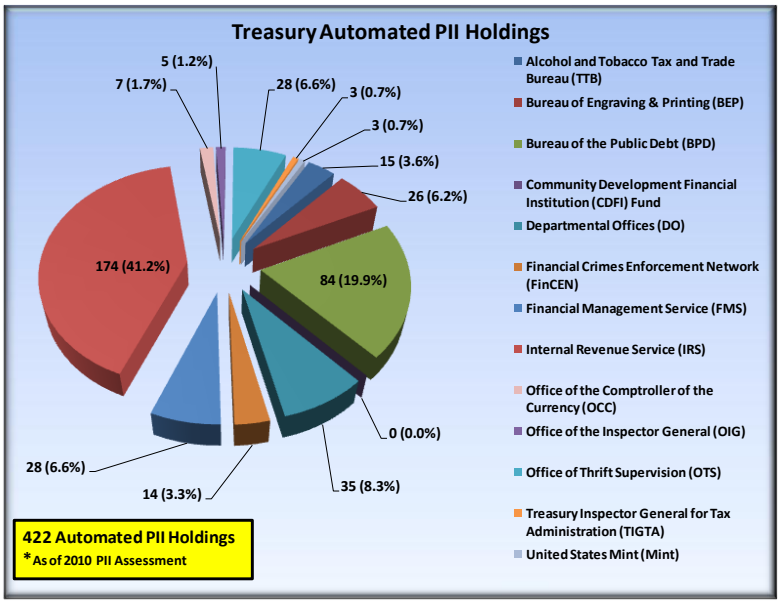

Figure 2 Treasury Automated PII Holdings

Figure 3 displays additional attributes about Treasury's PII holdings. Currently 114 automated systems contain PII on foreign nationals and 57 automated systems share data outside of the Department.

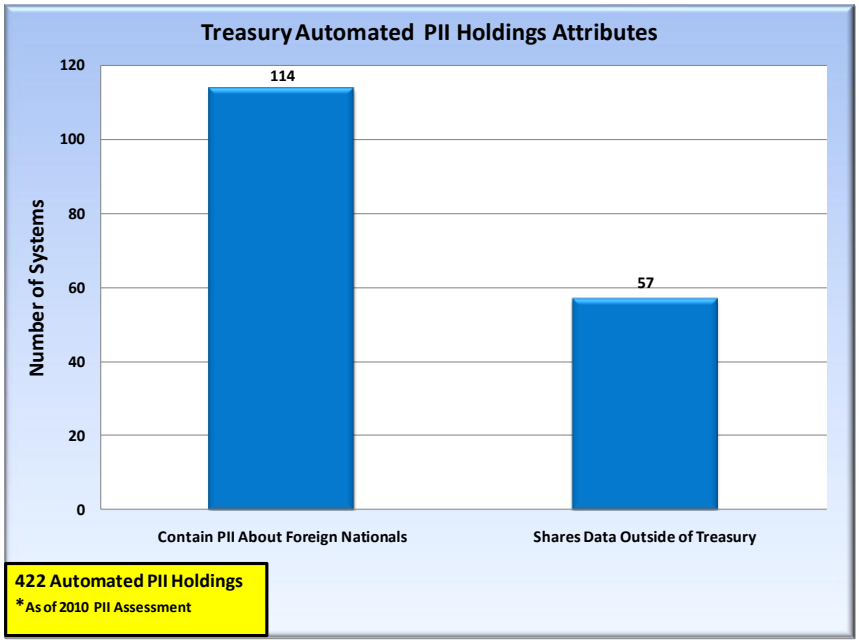

Figure 3 Treasury Automated PII Holdings Attributes

The locations of these automated systems containing PII are also very important to know. Due to the sensitivity of the information contained within these systems, the government should try to limit the amount of systems co-located at a contractor's site. **Figure 4** shows that a majority of the systems (85%) are located at a Treasury facility.

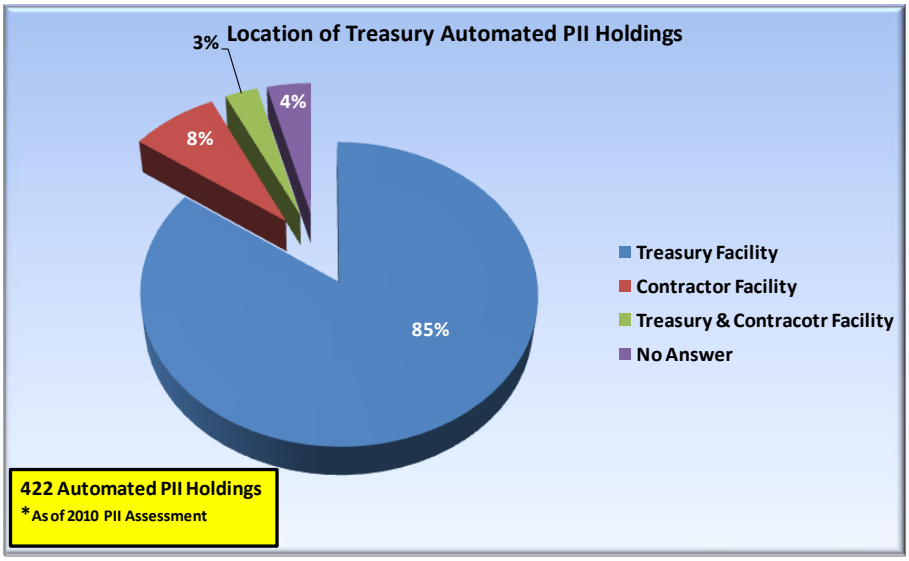

Figure 4 Location of Treasury Automated PII Holdings

b. Paper PII Holdings

In addition to automated systems, the assessment also identified the paper systems that contained PII across the Department. **Figure 5** displays that 153 paper systems containing PII exist across the Department. More than 80 percent of those systems reside within the BPD and the DO.

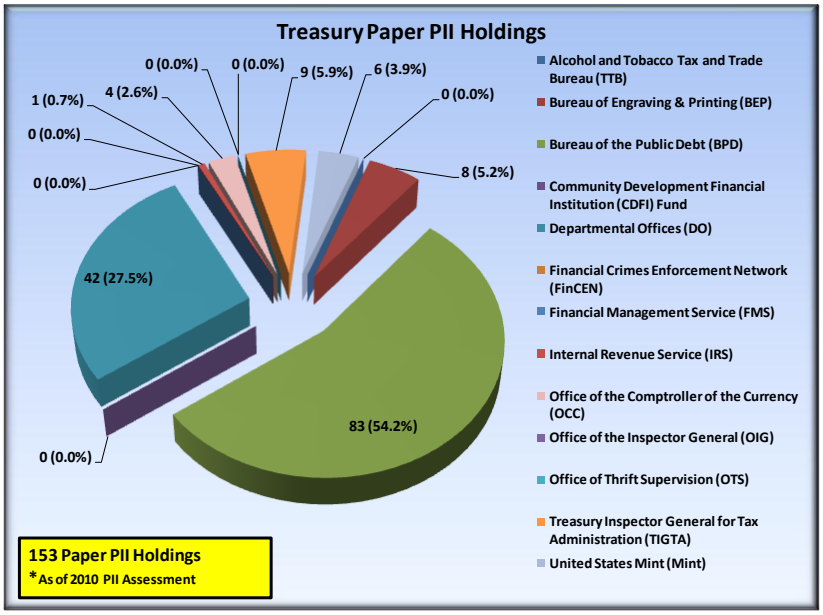

Figure 5 Treasury Paper PII Holdings

It should also be noted the DO and Bureaus reported that 35 percent (53) of their paper systems contain PII on foreign nationals.

The locations of these paper systems are also very important to know. **Figure 6** shows that a majority of the systems (95%) are located at a Treasury facility.

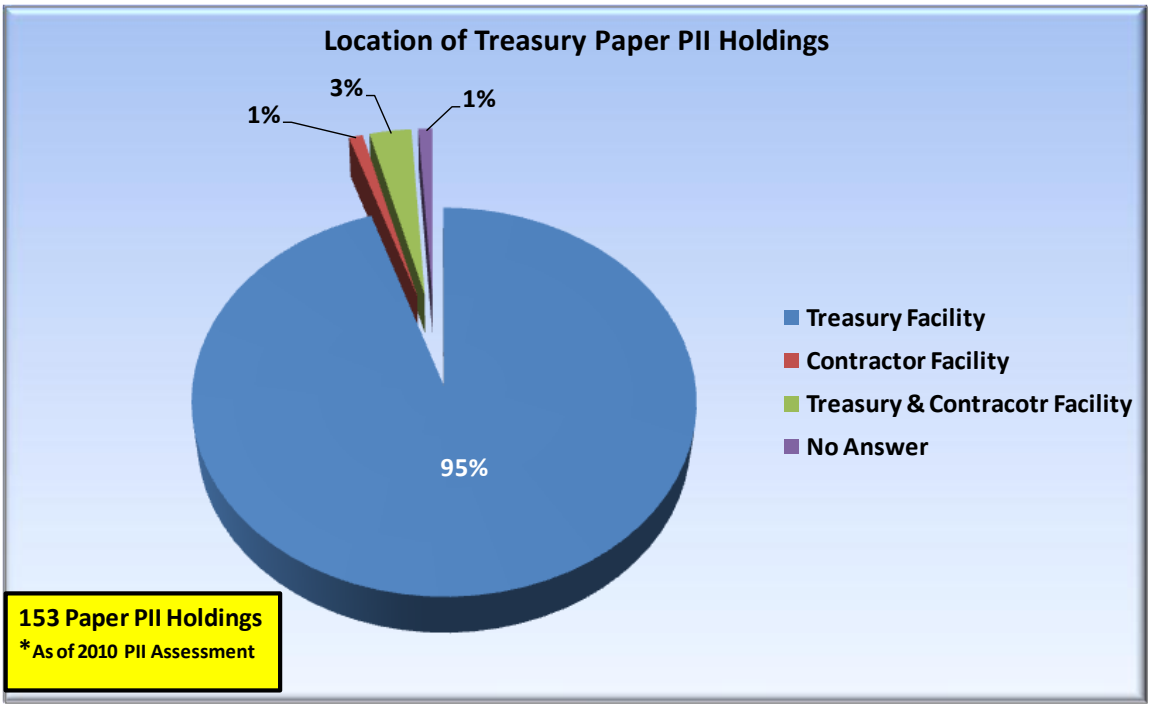

Figure 6 Location of Treasury Paper PII Holdings

2. SORNs Published

In FY 2010, OPCL published seven (7) SORNs to the *Federal Register*. Two (2) of the publications are compilations to cover Treasury wide and DO SORNs. The other publications were individual SORNs. Please refer to **Table 2** in **Appendix D** for the list of publications OPLC published to the *Federal Register*. Some of the SORNs published were new, while others were republished to the *Federal Register* to address systems that were altered. **Figure 7** displays the number of SORNs that OPCL has published over the last three fiscal years.

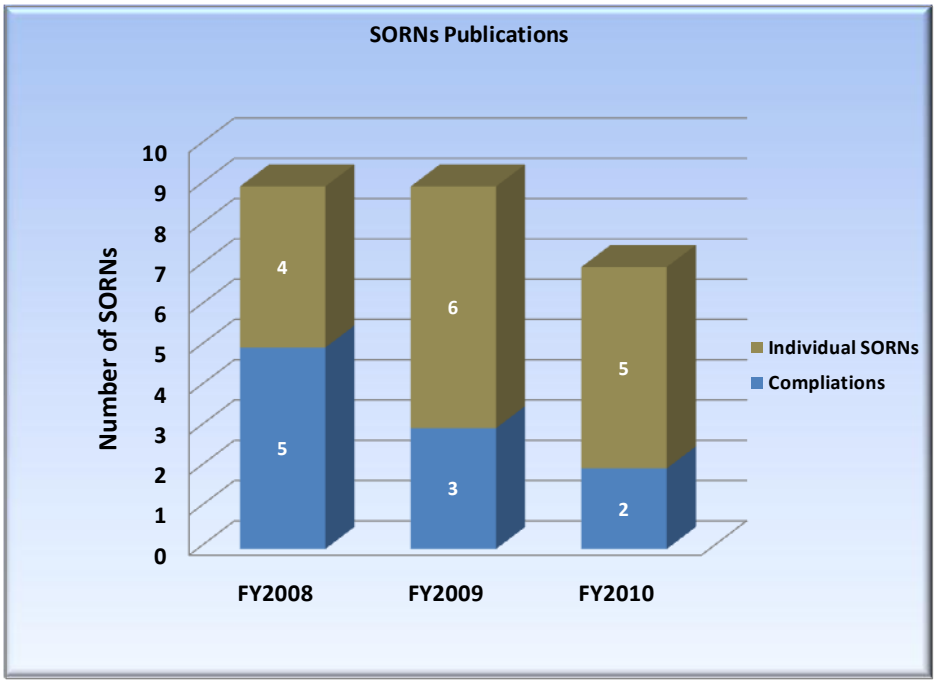

Figure 7 Published SORNs (FY 2008 – FY 2010)

3. FISMA Reporting

FISMA requires agency program officials, Chief Information Officers (CIOs), and Inspectors General (IGs) to conduct annual reviews of the agency's information security program and report the results to OMB. OMB uses this data to assist in its oversight responsibilities and to prepare this annual report to Congress on agency compliance with FISMA. To ensure privacy protections for PII, agencies are also required to report on performance metrics related to their privacy management programs. In addition to tracking the metrics for E-Government Act responsibilities, agencies are also required to report on additional metrics, including those associated with the Privacy Act (5 U.S.C. § 552a). As of the 4th quarter FY 2010, the Department reported a total inventory of 318 FISMA systems. **Figure 8** displays that out of the 318 systems reported for FISMA, 68 of the systems were not required to develop PIAs. The remaining 250 systems all had PIAs on file.

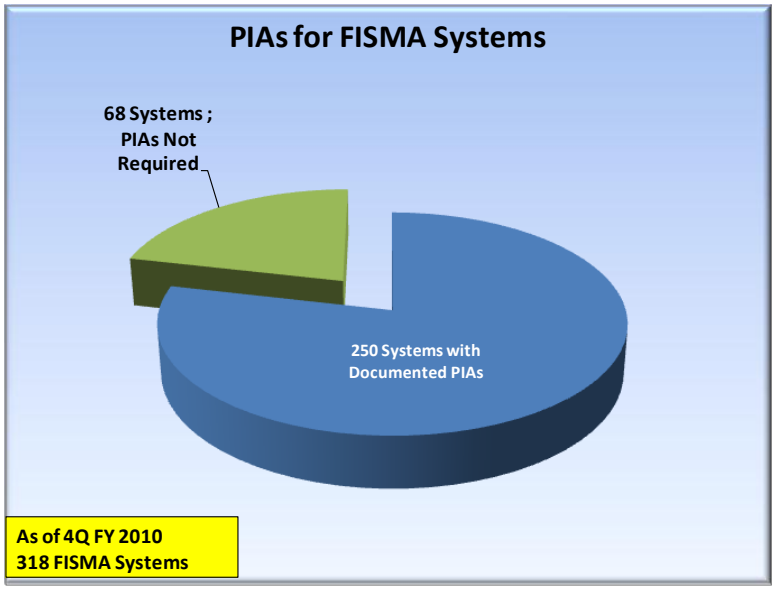

Figure 8 FY 2010 FISMA Reporting (PIAs)

Figure **Figure 9** illustrates that the Department has exceeded the threshold values for these metrics for the last three (3) years (FY 2008 – FY 2010).

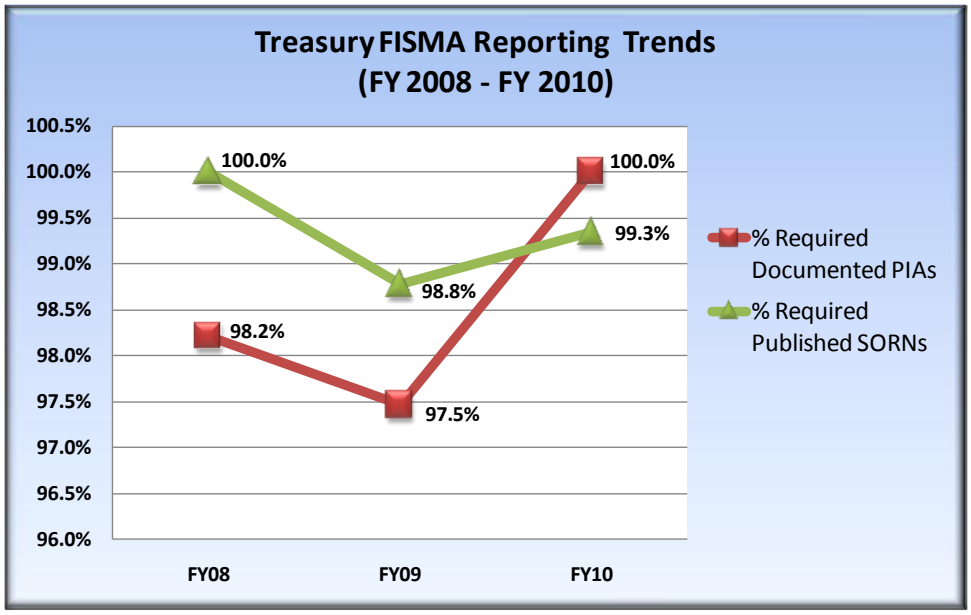

Figure 9 Treasury-Wide FISMA Reporting Trends (FY 2008 – FY 2010)

4. Section 803 Reporting

Each quarter, OPCL issues a data call in order to prepare the Department of the Treasury Report, Pursuant to Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007. The report highlights privacy and civil liberties activities and accomplishments under the

purview of the Chief Privacy and Civil Liberties Officer. The following is a description of the reporting categories for the Section 803 report:

- *Reviews*: Reviews include Treasury Department activities delineated by controlling authorities, such as the Privacy Act of 1974, 5 U.S.C. § 552a; E-Government Act of 2002 (P.L. 107-347); Consolidated Appropriations Act of 2005 (P.L. 108-447); OMB Circular A-130, Appendix 1; and OMB Memo M-07-16.
- *Advice and Response*: Advice and Response includes written policies, procedures, guidance, or interpretations of privacy requirements for circumstances or business processes that respond to privacy or civil liberties issues or concerns and the specific action taken in response to the advice given by the Department.

The report also addresses the types of complaints the DO and Bureaus received over the year. The following is a list of the type of complaints that are reported in Section 803:

- *Privacy Complaints*: A written allegation of harm or violation of personal or information privacy filed with the Treasury Department.
- *Civil Liberties Complaints*: A written allegation of harm or violation of the constitutional rights afforded individuals filed with the Treasury Department.

ODASPTR has continued to provide timely submissions of the Section 803 metrics to Congress on behalf of the Department**. Figure 10** displays the FY 2010 Section 803 report for the Department. For FY 2010 the department performed 457 reviews, provided advice and responses 113 times and responded to four (4) privacy and civil liberties complaints. Based on the data presented in **Figure** 10, it is evident that the majority of the activities by the DO and Bureaus had to deal with reviews and providing advice and responses.

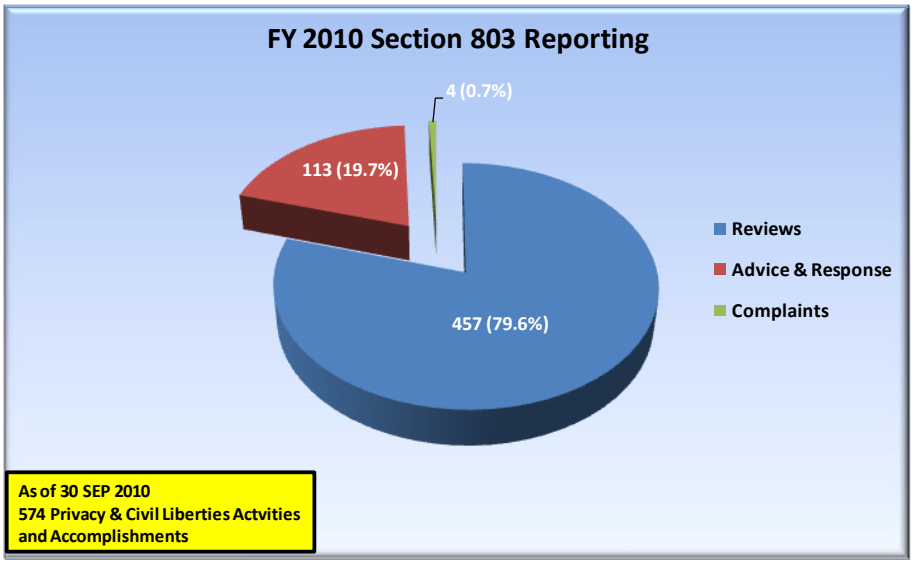

Figure 10 FY 2010 Section 803 Reporting

5. Privacy Awareness and Training

a. Mandatory Privacy Awareness Course

In FY 2010, OPCL launched a revised version of its mandatory privacy awareness training. DO employees were required to complete the mandatory privacy awareness-training course entitled, "A Culture of Privacy Awareness," by June 1, 2010. In addition to the standard course, OPCL created a test-out feature (per the Bureaus' requests) to allow employees to demonstrate their knowledge of privacy principles and practices. The staff also monitors and tracks the training progress within each bureau to ensure that bureaus meet our Department goal of 95 percent. The Department reported a 98 percent completion rate. The test-out feature will also be used in FY11 with new and improved questions.

Based on the feedback received from the OPCL Annual PII Assessment, OPCL initiated an update to the mandatory privacy annual awareness training in FY 2010. This update will help increase the privacy awareness of Treasury employees to ensure that the DO and Bureaus comply with the latest policies governing privacy and the handling of PII. The updated privacy awareness training will be completed and implemented by June 01, 2011.

b. Privacy Week

In order to increase the awareness of federal employees to the importance of privacy and the importance of correctly handling privacy related information, OPCL sponsored and planned a privacy week for the DO, Bureaus, and other federal agencies as a part of the ODASPTR Records and Information Management Month (RIMM). The dates for the event were from April 26, 2010 – April 30, 2010. Events included four individual speaker presentations, two panel discussions, two workshops and a privacy and security vendor fair. Speakers came from within Treasury as well as from other federal government agencies, and included several representatives

from privacy public interest groups. Approximately 700 participants registered for the week's events. The agenda included topics from data breach and identity theft to Web 2.0 technologies.

c. PII Breach Training

OPCL assisted the DASPTR in hosting an Interagency Data Breach Forum workshop on Wednesday, June 30, 2010. The workshop was an opportunity for Senior Agency Officials for Privacy (SAOP), Chief Privacy Officers (CPOs), Chief Information Officers (CIOs), managers, and analysts to participate in an interactive session designed to share best practices and identify opportunities to strengthen privacy practices and programs across the government. The workshop included sharing lessons learned and best practices, tabletop exercises simulating data breaches, and identifying opportunities for collaborative problem solving across agencies. The workshop concluded with a list of actions to take back to the Privacy Committee of the Federal CIO Council for follow-up. Eighty-five individuals participated, representing over 30 federal agencies.

B. Intra-agency Coordination

1. International Association of Privacy Professionals (IAPP)

The Department of Treasury relies on its employees as the first line of defense in protecting the public's PII from unauthorized uses or release. Treasury employs privacy officials that are responsible for ensuring that the DO and Bureaus are compliant with government privacy policies. Privacy practices and implementations are rapidly changing due to the way information is shared globally. This global sharing of information combined with the change in the technology landscape has increased information sharing not only amongst the different government agencies but also between different countries with differing privacy laws and policies.

In FY 2010, with DO and Bureaus' participation, OPCL was able to secure corporate membership with the International Association of Privacy Professionals (IAPP) for the Department of Treasury employees. IAPP is the world's largest association of privacy professionals. The partnership will provide Treasury with the opportunity of increasing the number of industry-certified professionals. This partnership will also allow Treasury professionals the opportunity to interact with the industries international privacy experts in a forum to share best practices, track trends, advance privacy management issues, standardize the designations for privacy professionals, and provide education and guidance on opportunities in the field of information privacy.

2. Treasury Information Privacy Council and Committee

a. Information Privacy Council

To gain Department-level support for privacy initiatives, the Treasury established the Information Privacy Council, which is comprised of senior executives who play a critical role in

the Department's privacy program. 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, who in turns advises the SAOP, 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 2010, 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.

b. 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 the 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 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, the Treasury privacy training efforts have been highly successful.

3. Treasury Computer Security Information Response Center (TCSIRC) Reporting

OPCL monitors the loss of PII across the Department, and makes recommendations for initiatives to reduce those losses, working through the DASPTR. Monthly statistics on these types of losses are collected, analyzed, and reported back to the DO and Bureaus for their consumption using the Treasury Computer Security Information Response Center (TCSIRC). OPCL is also responsible for the management of any breaches of data containing PII, and requires this data to support that effort. TCSIRC data was collected for FY 2010 and will be used as a baseline for future trending analysis. FY 2010 data is currently being analyzed. The outcome from this analysis will be used to provide recommendations to the SAOP of the best way to reduce the number of losses of PII across the Department. OPCL will start reporting on this metric in FY 2011

4. PII Risk Management Group (PIIRMG)

The PIIRMG is an executive-level, risk-management group, chaired by the SAOP, designed to assist the affected DO or Bureau in mitigating the impact of the breach as well as to identify opportunities to prevent breaches. 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 because of a PII breach.

C. Inter-agency Coordination

The CIO Council serves as a focal point for coordinating challenges that cross agency boundaries. CIO Council consists of six (6) committees: Accessibility, Architecture and Infrastructure, Best Practices, Information Security & Identity Management, IT Workforce, and Privacy. The DASPTR serves as the Treasury representative for the privacy committee.
The DASPTR serves as the Treasury representative for the privacy committee. The Privacy Committee is the principal interagency forum to improve agency practices for the protection of privacy. The Privacy Committee also serves as the interagency coordination group for SAOPs and CPOs in the federal government that provides a consensus-based forum for the development of privacy policy and protections throughout the federal government by promoting adherence to the letter and spirit of laws and best practices advancing privacy. The CIO Council Privacy Committee currently has four (4) standing subcommittees. OPCL staff members currently serve on all four (4) of the following subcommittees: Best Practices, Innovation and Emerging Technology, Development and Education, and International Privacy.

During FY 2010, OPCL supported the Information and Emerging Technology Subcommittee by taking part in a series of meetings to discuss issues dealing with privacy and the use of social media applications such as Facebook, Twitter, and YouTube on the Department's websites. Since the Treasury Department was new to the social media arena, the decision was made that

the Department would refrain from collecting any related PII via these third party social media applications. As policy continues to evolve dealing with the use of social media by the Federal Government, OPCL will revisit the issue to ensure that the entire Department remains in compliance with the latest policies.

In support of the Development and Education Subcommittee mission to serve as a forum for educating federal employees in the understanding, improving, and the application of privacy laws, regulations, policies, and procedures, the DASPTR co-chaired the 2010 Federal Privacy Summit. Additionally, OPCL also supported the subcommittee's efforts by opening its privacy week training to all federal agencies. Along with privacy week, OPCL also hosted a PII breach forum where over 30 federal agencies were represented and the OPCL continued its support of the International Privacy Subcommittee by providing input and speakers on the Department's activities dealing with the intersection of US and international privacy laws and practices.

D. Orders and Directives

Treasury Directives are documents signed by the appropriate senior Treasury officials that may further delegate authority from the most senior officials to other Treasury officials; and provide processes for implementing legal obligations and Departmental policy objectives. The following sections discuss the Treasury Directives OPCL either provided to publish or played a role in their development during FY 2010.

1. Treasury Directive (TD) 25-04

OPCL processed Treasury Directive 25-04, "Privacy Act." The TD was updated to reflect the new organization, and to provide clearer policy guidance. The Government Accountability Office (GAO) in its report (GAO-08-603, May 08) determined that a key privacy function, "redress" for violations, was not under the oversight of the Treasury Department's Senior Agency Official for Privacy (SAOP). The planned corrective action further revises the Directive to clarify that bureaus are to submit a copy of the initial determinations and responses to appeals regarding requests to amend records to the Office of the Deputy Assistant Secretary for Privacy and Treasury Records.

2. Treasury Directive (TD) 25-08

OPCL processed Treasury Directive 25-08, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information." This Directive establishes the Department's policy with respect to protecting PII, developing breach response and notification plans, and establishing the role of the Department's Personally Identifiable Information Risk Management Group (PIIRMG). It also addressed GAO Audit OIG -09-014 planned corrective action that was due for completion by December 31, 2009.

3. Departmental Offices (DO) Directive 305

In response to the ASM's efforts to make DO employees more accountable for loss of mobile electronic devices, particularly when containing PII, the Director of OPCL initiated Departmental meetings to discuss an effective approach to address the ASM's and SAOP's growing concerns about lost mobile IT assets. These meetings consisted of a set of discussions surrounding the most effective way to draft policy that would be comprehensive to all levels of employees and that could withstand labor management and union scrutiny. Based on these discussions, OPCL provided significant input to draft DO policy increasing accountability for lost mobile devices.

E. Other Significant Events

On July 21, 2010, President Obama signed the Dodd-Frank Wall Street Reform and Consumer Protection Act. The new law created multiple financial reform entities such as the Financial Stability Oversight Council (FSOC), the Office of Financial Research (OFR), the Federal Insurance Office (FIO), and the Bureau of Consumer Financial Protection (CFPB).
The FSOC is charged with identifying threats to the financial stability of the United States; promoting market discipline; and responding to emerging risks to the stability of the United States financial system. The OFR is responsible for supporting FSOCs mission by improving the quality of financial data available to policymakers and facilitating more robust and sophisticated analysis of the financial system. The FIO monitors all aspects of the insurance industry, including identifying issues or gaps in the regulation of insurers that could contribute to a systemic crisis in the insurance industry or the United States financial system. The CFPB is charged to protect and inform consumers of financial products, which by their nature can be too complex for non-professionals to understand.

As new entities, OPCL provides support by advising them on Departmental policies pertaining to the handling of PII. OPCL also assists the agencies in putting applicable SORNs and PIAs in place for new systems.

III. Privacy 2011 Outlook

A. Privacy Oversight and Compliance

With the increase and use of technology to promote and implement the President's initiative for Transparency and Open Government, ODASPTR and OPCL, in its role as the Department's lead in Privacy compliance and oversight, will continue to support the DO and Bureaus on all matters dealing with privacy related issues.

In FY 2011, OPCL will perform a follow on assessment of Treasury's PII Holdings. The assessment will be an update to the assessment that was performed in FY 2010, which established the baseline. The FY 2010 PII holdings assessment resulted in a list of lessons learned and recommendations that will be reviewed and implemented before the follow on

assessment in FY 2011. OPCL plans to update the assessment tool, with the aid of the DO and Bureaus, to ensure that their comments and concerns are addressed and fully adjudicated before an update to the assessment is completed in FY 2011. The updated tool will consist of updates to some of the questions in order to further increase awareness of PII and proper handling and the type of systems that need to be inventoried. The PII assessment in FY 2011 will also be executed electronically using a web based knowledge management system. DO and Bureau representatives will be able to update their information in real-time via the web based knowledge management tool resulting in a less laborious process as compared to the previous year.
In FY 2011 OPCL will support the development and implementation of ODASPTR's Enterprise Content Management (ECM) initiative. OPCL will support the ECM initiative by reviewing plans, documentation, and advising on whether a PIA is needed for the ECM system or the cloud-based solution for Electronic Freedom of Information Act (eFOIA). OPCL will also provide support to ensure the e-content is appropriately received to minimize PII, and the proper procedures are in place to correctly handle and protect necessary PII safely.

B. Intra-Agency and Inter-Agency Coordination

With the flow of information into cyberspace becoming increasingly "borderless", there is a need to identify where privacy laws and expectations both intersect and diverge on an international scale. In FY 2011, the DASPTR will co chair, and OPCL will continue to support the International Privacy Subcommittee's efforts to provide a forum to address the intersection of the U.S privacy and data protection laws and the international communities' privacy standards and laws. The subcommittee will continue to address issues surrounding the perception that U.S. data privacy laws are inadequate when privacy rights of Non-U.S. citizens are at issue. Treasury representatives will also continue to support the subcommittee's work as an inter-agency forum for agencies that have an interest in the U.S. government's privacy framework and international data privacy standards and developments. These efforts will help adjudicate and bridge the gap between the U.S. Government and the international communities' privacy laws and standards.
OPCL will also continue to participate in additional intra-agency and interagency forums in order to monitor, disseminate, or develop new or updated policy for the Department. OPCL will also continue to adjudicate any issues that the DO and Bureaus have with implementing any policies dealing with privacy related issues.

C. Privacy Awareness and Training

OPCL also plans to update the annual privacy training in FY 2011. The update will consist of better scenarios and provide more details and understating of what constitutes PII. The goal is to increase the DO and Bureau employees' awareness and recognition of PII and its proper handling. OPCL will also investigate and develop additional initiatives that will support its goal to embed training throughout the Department.

IV. Appendices

Appendix A List of Acronyms

ASM/CFO	Assistant Secretary for Management and Chief Financial Officer
CIO	Chief Information Officer
CPCLO	Chief Privacy and Civil Liberties Officer
CPO	Chief Privacy Officer
DAS	Deputy Assistant Secretary
DASPTR	Deputy Assistant Secretary Privacy, Transparency, and Records
DO	Departmental Offices
eFOIA	Electronic Freedom of Information Act
ECM	Enterprise Content Management
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 Council/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 Privacy, Transparency, and Records
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OPCL	Office of Privacy and Civil Liberties
OPTR	Office of Privacy, Transparency, and Records
PCLOB	Privacy and Civil Liberties Oversight Board
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIIRMG	PII Risk Management Group
PTA	Privacy Threshold Analysis
RIMM	Records and Information Management Month
SAOP	Senior Agency Official for Privacy
SIGTARP	Special Inspector General for Troubled Asset Relief Program
SOR	System of Records
SORN	Systems of Records Notices
TARP	Troubled Asset Relief Program

TCSIRC	Treasury Computer Security Information Response Center
TD	Treasury Directive
TIGTA	Treasury Inspector General for Tax Administration

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

1. **31 CFR Part 1, Treasury privacy regulations**
2. **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)
3. **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)
4. **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
5. **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)
6. **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)
7. **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)
8. **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.
9. **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)
10. **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.)

11. **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)
12. **National Institute of Standards and Technology (NIST) Standards Publication (SP) 800-122 (Draft)**, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
13. **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.
14. **OMB M-99-05** provides instructions for complying with President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records"
15. **OMB M-05-08**, Designation of Senior Agency Officials for Privacy
16. **OMB M-06-15**, Safeguarding Personally Identifiable Information
17. **OMB M-06-16**, Protection of Sensitive Agency Information
18. **OMB M-06-19**, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments
19. **OMB Memo Sept. 20, 2006**, Recommendations for Identity Theft Related Data Breach Notification
20. **OMB M-07-16**, Safeguarding Against and Responding to the Breach of Personally Identifiable Information
21. **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
22. **OMB M-08-21**: FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
23. **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)
24. **Section 803 of the Implementing the Recommendations of the 9/11 Commission Act of 2007**, P.L. No. 110-53
25. **Treasury Order 102-25**, Delegation of Authority Concerning Privacy and Civil Liberties
26. **Treasury Directive 25-04**, Privacy Act of 1974, (reflects OPTR as a new organization, provides clearer guidance, and address GAO redress concerns)
27. **Treasury Directive 25-07**, Privacy Impact Assessment (PIA), (provides guidance to Treasury Bureaus on determination and completion of PIAs)
28. **Treasury Directive 25-08**, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII)

29. **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 Department of Treasury Bureaus and Offices

1. Bureau of Engraving and Printing (BEP)
2. Bureau of Public Debt (BPD)
3. Community Development Financial Institutions (CDFI)Fund
4. Departmental Offices (DO, also known as Headquarters)
5. Financial Crimes Enforcement Network (FinCEN)
6. Financial Management Service (FMS)
7. Internal Revenue Service (IRS)
8. United States Mint (Mint)
9. Office of the Comptroller of the Currency (OCC)
10. Office of the Inspector General (OIG)
11. Office of Thrift Supervision (OTS)
12. Special Inspector General for TARP (SIGTARP)
13. The Alcohol and Tobacco Tax and Trade Bureau (TTB)
14. Treasury Inspector General for Tax Administration (TIGTA)

Appendix D Reference Tables

Table 2 FY 2010 Published SORNs

Title	Date	Published
PA Compilations		
Treasury-wide Privacy Act System of Records	9/7 /10	75 FR 54423
DO System of Records - Compilation	4/30/10	75 FR 20676
New/Altered PA Notices Published		
BEP .048 - Electronic Police Operation Command Reporting System (EPOCRS)	8/25/10	75 FR 52394
Alteration: - DO .218 - Home Affordable Modification Program	7/2/10	75 FR 38608
New SIGTARP Notices: SIGTARP/DO .220 - .224	1/14/10	75 FR 2188
BEP 006 - Debt Files (Employees) Alteration	12/30/09	74 FR 69190
Final notice - DO .218 - Home Affordable Modification Program	10/28/09	74 FR 55621

Table 3 FY 2010 Number of Department of Treasury PII Holding

Organization	Automated	Paper
Alcohol and Tobacco Tax and Trade Bureau (TTB)	15	0
Bureau of Engraving & Printing (BEP)	26	8
Bureau of the Public Debt (BPD)	84	83
Community Development Financial Institution (CDFI) Fund	0	0
Departmental Offices (DO)	35	42
Financial Crimes Enforcement Network (FinCEN)	14	0
Financial Management Service (FMS)	28	0
Internal Revenue Service (IRS)	174	1
Office of the Comptroller of the Currency (OCC)	7	4
Office of the Inspector General (OIG)	5	0
Office of Thrift Supervision (OTS)	28	0
Treasury Inspector General for Tax Administration (TIGTA)	3	9
United States Mint (Mint)	3	6
Subtotal	422	153
Total		575

Appendix E List of Figures

FIGURE 1 TREASURY PII SYSTEMS RELATIONSHIPS 5
FIGURE 2 TREASURY AUTOMATED PII HOLDINGS 5
FIGURE 3 TREASURY AUTOMATED PII HOLDINGS ATTRIBUTES 6
FIGURE 4 LOCATION OF TREASURY AUTOMATED PII HOLDINGS 6
FIGURE 5 TREASURY PAPER PII HOLDINGS 7
FIGURE 6 LOCATION OF TREASURY PAPER PII HOLDINGS 8
FIGURE 7 PUBLISHED SORNS (FY 2008 – FY 2010) 9
FIGURE 8 FY 2010 FISMA REPORTING (PIAS) 10
FIGURE 9 TREASURY-WIDE FISMA REPORTING TRENDS (FY 2008 – FY 2010) 10
FIGURE 10 FY 2010 SECTION 803 REPORTING 12

Appendix F List of Tables

TABLE 1 OPCL'S COMPLIANCE PERFORMANCE MEASURES 3
TABLE 2 FY 2010 PUBLISHED SORNS D-1
TABLE 3 FY 2010 NUMBER OF DEPARTMENT OF TREASURY PII HOLDING D-2