Department of the Treasury

2011 - 2012 Privacy Report to Congress

MESSAGE FROM THE CHIEF PRIVACY AND CIVIL LIBERTIES OFFICER

As required by Section 522 of the Consolidated Appropriations Act of 2005, I am pleased to present the Department of the Treasury's Privacy Report for Fiscal Years 2011 and 2012. Over the past two years, Treasury's privacy program has undergone significant changes to enable it to provide improved services to Treasury, the public, and the federal government community. This report focuses on these changes, the program's achievements in Fiscal Years 2011 and 2012, and the goals for Fiscal Year 2013.

Inquiries about this report may be directed to the Treasury Office of Privacy, Transparency, and Records at privacy@treasury.gov. This report, as well as previous Annual Reports, can be found on the Department's Privacy Act website at www.treasury.gov/privacy.

/s/
Nani Coloretti
Assistant Secretary for Management
Senior Agency Official for Privacy & Chief Privacy and Civil Liberties Officer
Department of the Treasury

EXECUTIVE SUMMARY

The Department of the Treasury (Treasury or Department) Office of Privacy, Transparency, and Records' (OPTR) mission is to serve the public and the Federal Government community by setting the standard for protecting, retaining, preserving, disclosing and allowing access to Treasury's information. OPTR continuously strives to improve performance in each of these areas. This report, covering the period from October 1, 2010, through September 30, 2012, catalogues OPTR's continued success in monitoring and overseeing privacy compliance throughout the Department.

Treasury's privacy program starts with the idea that every employee is responsible for protecting personally identifiable information (PII). To ensure everyone is aware of their responsibilities, OPTR works hard to make sure each employee receives the Department's Culture of Privacy Awareness Training. For Fiscal Years (FY) 2011 and 2012, approximately 98 percent of all Treasury employees, contractors, and consultants successfully completed their annual privacy awareness training.

In addition to training Treasury's employees, OPTR constantly seeks opportunities to improve the Department's policies and procedures for ensuring privacy and safeguarding PII. In FY 2011 and 2012, OPTR drafted two Treasury Directives: *Information Sharing Environment Privacy and Civil Liberties Policy* and *Using Social Media Websites Information Sharing Environment Privacy and Civil Liberties Policy*. It is expected that they will be finalized and published in FY 2013 or early in FY 2014.

During the period of this report, the Department successfully carried out a number of initiatives that have fundamentally changed the way it conducts its daily privacy activities. Perhaps the two most significant initiatives were the Department's hugely successful PII inventory initiative and the Enterprise Content Management (ECM) initiative.

In FY 2011 and 2012, OPTR conducted a thorough inventory of its PII holdings and identified every system, both automated and paper-based, containing PII. With the completion of the PII holdings survey, Treasury is not only in full compliance with the Office of Management and Budget (OMB) M-07-16 mandate, but it also has a sound knowledge and understanding of the breadth and depth of the PII entrusted to its care. Using this information, OPTR intends to work with the bureaus and Departmental Offices to reduce the Department's PII holdings by identifying systems containing PII that can potentially be eliminated.

ECM is the vehicle by which Treasury organizes, stores, and manages its documents. In FY 2012, OPTR leveraged the ECM platform and initiated an effort to streamline the creation, review, and approval of privacy impact assessments (PIA). By modifying the technology used by the preexisting departmental Clearance Tracker to comport with the PIA clearance process, the Department and its bureaus will be able to process and track PIAs, thereby enhancing the efficiency of Treasury's PIA development and review process.

A principal reason for the success of Treasury's privacy program is the close collaboration between OPTR, the Office of Chief Information Officer (OCIO), and all of Treasury's bureaus and Departmental Offices. OPTR works closely with the Department's bureaus and Departmental Offices on a daily basis to develop and implement appropriate policies to address PII issues that arise in executing the Department's mission. Additionally, OPTR and OCIO work collectively to implement the mandates in Section 522 of the Consolidated Appropriation Act of 2005, the Federal Information Security Management Act of 2002 (FISMA), and Section 208 of the E-Government Act of 2002, as well as a significant body of applicable privacy law and policy. This collaborative effort is a key contributor to the Department's overall success in protecting PII.

2011 - 2012 Privacy Report to Congress

TABLE OF CONTENTS

LEGISLATIVE LANGUAGE

This report has been prepared in accordance with Section 522(a) of the Consolidated Appropriations Act of 2005, which includes the following requirement:

Privacy Officer—

> Each agency shall have a Chief Privacy Officer to assume primary responsibility for privacy and data protection policy, including—
>
> * * *
>
> (6) preparing a report to Congress on an annual basis on activities of the Department that affect privacy, including complaints of privacy violations, implementation of section 552a of title 5, 11 United States Code, internal controls, and other relevant matters;
>
> * * *

BACKGROUND

The Chief Privacy and Civil Liberties Officer and Senior Agency Official for Privacy

Section 522 of the Consolidated Appropriations Act of 2005 requires the Department of the Treasury (Treasury or Department) to appoint a Chief Privacy Officer (CPO) to assume primary responsibility for privacy and data protection policy. Similarly, Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007 requires the Department to appoint a senior officer to serve as the Department's Privacy and Civil Liberties Officer (PCLO).

In addition to the statutory requirements to appoint a CPO and PCLO, the Office of Management and Budget (OMB) issued Memorandum 05-08, *Designation of Senior Agency Officials for Privacy*, which directs agency heads to designate a Senior Agency Official for Privacy (SAOP) with agency-wide responsibility for ensuring the agency's implementation of information privacy protections and full compliance with information privacy laws, regulations, and policies.

Consistent with these requirements, 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*, combines the responsibilities associated with the CPO and PCLO positions and assigns them to a Chief Privacy and Civil Liberties Officer (CPCLO). The Department's Assistant Secretary for Management (ASM) serves as the CPCLO. The ASM is also designated as the SAOP by TD 25-04, *The Privacy Act of 1974, As Amended*.

Pursuant to Section 522(a) of the Consolidated Appropriations Act of 2005, the ASM, as CPO, is responsible for:

(1) assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of information in an identifiable form;
(2) assuring that technologies used to collect, use, store, and disclose information in identifiable form allow for continuous auditing of compliance with stated privacy policies and practices governing the collection, use and distribution of information in the operation of the program;
(3) assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as defined in the Privacy Act of 1974;
(4) evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government;
(5) conducting a privacy impact assessment of proposed rules of the Department on the privacy of information in an identifiable form, including the type of [PII] collected and the number of people affected;
(6) preparing a report to Congress on an annual basis on activities of the Department that affect privacy, including complaints of privacy violations, implementation of section 552a of title 5, 11 United States Code, internal controls, and other relevant matters;
(7) ensuring that the Department protects information in an identifiable form and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction;

(8) training and educating employees on privacy and data protection policies to promote awareness of and compliance with established privacy and data protection policies; and
(9) ensuring compliance with the Department's established privacy and data protection policies.

Pursuant to the PCLO requirements under Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007, the ASM, as PCLO, is responsible for:

(1) assisting the head of such department, agency, or element and other officials of such department, agency, or element in appropriately considering privacy and civil liberties concerns when such officials are proposing, developing, or implementing laws, regulations, policies, procedures, or guidelines related to efforts to protect the Nation against terrorism;
(2) periodically investigating and reviewing department, agency, or element actions, policies, procedures, guidelines, and related laws and their implementation to ensure that such department, agency, or element is adequately considering privacy and civil liberties in its actions;
(3) ensuring that such department, agency, or element has adequate procedures to receive, investigate, respond to, and redress complaints from individuals who allege such department, agency, or element has violated their privacy or civil liberties; and
(4) considering certain factors when providing advice on department, agency, or element proposals to retain or enhance a particular governmental power, including whether the proponent has established—
    a. that the need for the power is balanced with the need to protect privacy and civil liberties;
    b. that there is adequate supervision of the use by such department, agency, or element of the power to ensure protection of privacy and civil liberties; and
    c. that there are adequate guidelines and oversight to properly confine its use.

Pursuant to OMB M-05-08, *Designation of Senior Agency Officials for Privacy*, the ASM, as SAOP, is responsible for:

(1) reviewing and updating privacy procedures;
(2) ensuring implementation of information privacy protections, including compliance with applicable information privacy laws, regulations, and policies;
(3) ensuring employees and contractors receive privacy training;
(4) having a role in Treasury's development and evaluation of legislative, regulatory, and other policy proposals that implicate information privacy issues.

To assist the ASM with the aforementioned responsibilities, TD 25-04 designates the Deputy Assistant Secretary for Privacy, Transparency, and Records (DASPTR) as her principal advisor on issues related to privacy and civil liberties. The DASPTR oversees the protection, access, and disclosure of Treasury's information assets and ensures that information the Department collects is maintained in a manner consistent with legal and policy requirements. The Office of Privacy and Civil Liberties (OPCL) is a component of OPTR and the OPTR unit directly involved in the subject matter of this report.

For the Department to meet its mission requirements, it must acquire and collect PII from the public, as well as from various organizations and other government agencies. The Department is responsible for managing and protecting the information it retains, uses, shares and discloses. These information management functions are regulated by federal laws, regulations and policies that are primarily designed to ensure government agencies maintain the public's trust while using PII.

OPTR's mission (working in conjunction with the Office of General Counsel and the Office of the Chief Information Officer) is to serve the Department, the public, and the Federal Government community. This entails continuously interacting with all Treasury components to provide information management services and ensuring that Treasury complies with the legal, regulatory, and policy requirements that govern information management. Compliance with these requirements is essential to preserving the public trust, without which the Department would not be able to get the information necessary to fulfill its various missions. Additionally, OPTR's support ensures that program offices may concentrate on their core functions.

OPTR is responsible for monitoring and overseeing privacy compliance throughout the Department. This includes working closely with Treasury managers to develop, implement, and monitor agency-wide privacy policies and procedures in compliance with the United States Constitution and relevant federal statutes, Executive Orders, OMB memoranda and guidance, as well as other relevant standards and regulations.

The DASPTR provides the ASM with day-to-day support in executing the privacy and civil liberties duties entrusted to her in her capacity as the Department's CPCLO and SAOP.

PRIVACY AWARENESS AND TRAINING

A Culture of Privacy Awareness

OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, requires agencies to train employees on their privacy and security responsibilities before granting them access to agency information and information systems. Additionally, agencies must provide at least annual refresher training to ensure employees continue to understand their responsibilities.

In FY 2011 and 2012, OPTR updated the departmental course "A Culture of Privacy Awareness" to include lessons learned during the first Treasury annual PII assessment, guidance on the use of social media, as well as other guidance related to protecting PII. Specifically, the requirements of OMB M-10-23, *Guidance for Agency Use of Third-Party Websites and Application*s, were added along with more examples of the types of PII found in Treasury employees' everyday work environment. In addition, to make the training more interactive, OPTR added questions throughout the training to have employees apply the concepts as they are being learned. Every year, OPTR updates the training to add new guidance and address issues that arose during the previous fiscal year.

All of the Department's bureaus and Departmental Offices, with the exception of the Internal Revenue Service (IRS) and the Office of the Comptroller of the Currency (OCC), use the departmental course. IRS and OCC employ their own training that addresses the core issues addressed in the departmental version of the training, but is also specifically tailored to their individual missions.

OPTR staff monitors and tracks the training progress across the Department to ensure an excellent completion percentage. For FY 2011 and FY 2012, 98 percent of all Treasury employees completed the annual privacy awareness training as required.

Privacy Awareness Orientation

In FY 2011, OPTR provided in-person privacy awareness training to new hires. The training included an overview of privacy and information privacy as well as the various laws, regulations, and guidance governing information privacy, the fair information practices principles, and the obligation of all federal employees to protect PII. In FY 2012, concerned about the overall length of orientation briefings, Treasury replaced in-person privacy awareness training with on-line training through the Department's Training Learning Management System (TLMS).

Support for Treasury Privacy Professionals

To increase access to additional privacy resources and improve the professional knowledge of Treasury's privacy community, OPTR maintains a corporate membership with the International Association of Privacy Professionals (IAPP) on behalf of the bureaus and Departmental Offices. The corporate membership provides member benefits for up to 150 Treasury privacy

professionals, including daily news from the privacy world, webcasts, conferences, various educational events, and the opportunity to interact with other industry experts at the annual IAPP Global Privacy Summit.

In FY 2012, OPTR coordinated a three-day, government-wide training session for employees registered for the IAPP'S Certified Information Privacy Professional (CIPP) exams. The CIPP exams cover U.S. privacy laws and regulations as well as more general privacy and data security subject matter and passing them is required to receive IAPP certification. OPTR recruited privacy and security experts from various federal agencies to serve as trainers. The government-wide training for privacy professionals resulted in more than 60 federal employees from 13 federal agencies sitting for the May 2012 training and June 2012 CIPP exams. Treasury currently has 43 employees who are CIPPs.

OVERSIGHT AND COMPLIANCE

System of Records Notices (SORN)

The Privacy Act of 1974, as amended (Privacy Act), 5 U.S.C. § 552a, governs federal agencies' collection, maintenance, use, and disclosure of personal information about an individual that is contained within a system of records. Pursuant to 5 U.S.C. § 552a (e)(4), agencies are required to publish systems of records notices in the *Federal Register*.

A system of records is a group of paper or electronic records maintained by a federal agency from which information about an individual is retrieved by the name of the individual or an identifying number, symbol, or other particular (e.g., Social Security number) assigned to the individual. Treasury has published regulations describing how it maintains, collects, uses, and disseminates records about individuals. These regulations provide procedures by which individuals may request access to their information that is maintained by Treasury. *See* 31 C.F.R. §§ 1.20-1.36.

From October 1, 2010, through September 30, 2012, the Department published 30 SORNs in the *Federal Register*. Two of the publications cover new Treasury-wide and DO SORNs. The other publications were alterations to individual bureau SORNs.

Treasury maintains approximately 305 systems of records, nearly 60 percent of which are maintained by the IRS. A complete list of the Department's SORNs is available online through the Privacy Act page at: www.treasury.gov/privacy.

Privacy Impact Assessments (PIA)

Section 208 of the E-Government Act of 2002 (E-Gov Act) requires agencies to conduct PIAs for electronic information systems and collections that involve the collection, maintenance, or dissemination of information in identifiable form from or about members of the public. Pursuant

to the E-Gov Act, agencies are required to make PIAs publicly available through the agency website, the Federal Register, or other means.

TD 25-07, *Privacy Impact Assessment*, sets the policy, procedures, and responsibilities for conducting and reporting on PIAs. Corresponding guidelines provided in Treasury Directive Publication (TD P) 25-07, *PIA Manual*, set the policy for conducting a PIA when developing or procuring information technology systems or projects that collect, maintain, or disseminate information that is in an identifiable form from or about members of the public.

Table 1: Compliance Performance Measures for FY 2011 and FY 2012

Performance Measure	Definition	Percentage Completed
Percent of SORNs Published	Percent of systems identified as requiring SORNs that have one published in the Federal Register	100
Percent of PIAs completed	Percent of systems identified as requiring a PIA that have one	100

PIAs are an invaluable tool for helping Treasury establish public trust while ensuring it continues to get the information needed to fulfill its mission. From October 1, 2010, through September 30, 2012, OPTR reviewed numerous PIAs. A list of the Department's PIAs is available online through the Privacy Act page at: www.treasury.gov/privacy. PIAs not accessible online are made available to members of the public upon request.

DEPARTMENT OF THE TREASURY DIRECTIVES

Department of the Treasury Directives (TDs) outline departmental policy objectives as well as the roles, responsibilities, and processes for implementing legal and policy obligations. In FY 2011 and 2012, OPTR began drafting a TD to address the Information Sharing Environment (ISE). OPTR also worked with the OCIO to develop a policy regarding the use of social media.

Proposed Treasury Directive 25-10: Information Sharing Environment Privacy and Civil Liberties Policy

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) created the ISE, which creates a process and structure for the sharing of information related to terrorism, weapons of mass destruction, and homeland security that is needed to enhance national security. The Program Manager for the Information Sharing Environment released the ISE Privacy Guidelines. These, in turn, require participating agencies to develop and implement written ISE privacy and civil liberties protection policies that sets forth the procedures its personnel will follow to implement the Guidelines.

Treasury is committed to maximizing the sharing of terrorism-related information while protecting information privacy and other legal rights. In FY 2011 and 2012, OPTR drafted TD 25-10, which will assist Treasury in implementing ISE privacy and civil liberties requirements. It is expected that the TD will be finalized and published in FY 2013.

Treasury Policy on Social Media: Ensuring Compliance with Privacy and Records Management Requirements When Using Social Media Websites

In FY 2011 and 2012, OPTR worked with the OCIO to draft a policy on social media use in the Department. This policy will provide Treasury-wide guidance on social media to ensure official use complies with privacy, records management, and information security requirements. This effort takes into account OMB's publication of M-10-22, *Guidance for Online Use of Web Measurement and Customization Technologies,* and M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications*. OMB issued guidance to ensure compliance with federal law and policy while at the same time also encouraging federal agencies to use social media to make government initiatives more open and transparent. In establishing a presence on social media websites, the Department must assess the inherent risks of operating in third-party environments. Once completed, this policy will provide guidance on reducing these risks. It is anticipated that the policy will be finalized and published in the fourth quarter of FY 2013 or early in FY 2014.

PII HOLDINGS ASSESSMENT

OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, requires agencies to "review their current holdings of all [PII] and ensure, to the maximum extent practicable, such holdings are accurate, relevant, timely, and complete, and reduce them to the minimum necessary for the proper performance of a documented agency function. . . . Following this initial review, agencies must develop and make public a schedule by which they will periodically update the review of their holdings."

In FY 2011, OPTR completed its initial assessment of Treasury's PII holdings. The assessment identified over 400 automated systems and nearly 150 paper-based systems containing PII. Using the information collected during the assessment, and with the support of OCIO, OPTR developed its PII Holdings Database (PII DB). OPTR will use the PII DB to manage the data collected from the initial review and as an assessment tool for annual reviews going forward.

In FY 2012, two questions were added to the assessment, one regarding systems that hold terrorism-related data and a second regarding systems that are included in annual FISMA reporting. OPTR intends to use the information it collects in response to these two questions to identify bureaus and offices that it needs to work with as it implements the requirements of the ISE. In addition, it is anticipated that this information will assist in FISMA reporting in 2013 and beyond.

Going forward, OPTR intends to reduce the Department's PII holdings by working with the bureaus and Departmental Offices to identify systems that can potentially be eliminated. OPTR will also assess ways to enhance the PII DB and to provide the bureaus more support in managing and safeguarding their PII holdings.

LEADERSHIP AND COORDINATION WITHIN TREASURY

Treasury Information Privacy Council and Information Privacy Committee

To promote information sharing and collaboration, Treasury established an Information Privacy Council (IP Council) and an Information Privacy Committee (IP Committee). The IP Council is comprised of senior executives who play a critical role in the Department's privacy program and is chaired by the DASPTR. The IP Committee consists of staff level employees who work on privacy initiatives as part of their daily functions. In FY 2011, the IP Council and IP Committee combined their meetings to create a collaborative forum where information is disseminated and relevant privacy issues and information are shared and discussed.

During FY 2011 and 2012, the IP Council and IP Committee elevated awareness of the risks and rewards of third-party websites and applications. There was a focus on OMB M-10-22, *Guidance for Online Use of Web Measurement and Customization Technologies*, and M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications*, which led to a better understanding of the consequences of using these technologies. Additionally, there were active discussions of other topics, such as National Institute of Standard Technology (NIST) SP 800-53 Appendix J, the implications of EINSTEIN 3A, and Department's participation in the ISE.

Treasury Computer Security Information Response Center (TCSIRC)

The Treasury Computer Security Information Response Center (TCSIRC) is the single organizational point of contact for computer security incident reporting. It is responsible for reporting incidents to the OCIO, Chief Information Security Officer, and reporting computer security incidents involving PII to OPTR. OPTR works closely with the TCSIRC to monitor PII risks across the Department and makes recommendations to reduce those losses and improve reporting processes.

During FY 2012, OPTR began working with TCSIRC employees to improve the quality of the incident reports. As a result of these efforts, the incident reporting form used by the Departmental Offices helpdesk was redesigned to increase the uniformity and accuracy of reports submitted by individuals reporting incidents. By redesigning the reporting form to add additional questions, OPTR was able to greatly reduce the resources dedicated to investigations after the initial incident report is submitted to the helpdesk.

Data Integrity Board

Pursuant to the Computer Matching and Privacy Protection Act of 1988 (CMPPA), each agency that participates in a matching program is required to establish a Data Integrity Board (DIB) to oversee the agency's participation in the program. Matching programs provide a direct benefit to the public by assisting in the elimination of errors and in monitoring waste, fraud, and abuse. Treasury's DIB evaluates proposed matching programs and approves the terms of required matching agreements before any component of Treasury participates in such a program.

In 2011, the CMPPA functions were organizationally placed under the OCIO. In 2012, these responsibilities were transferred to OPTR. These functions are now under the guidance of the Department's Privacy Act Officer. The Privacy Act Officer serves as a permanent member of the DIB, acts as the secretary to the Board, and maintains the minutes of Board meetings. The Department's Privacy Act Officer is also responsible for policy guidance and direction on privacy protection matters with respect to computer matching and implementing sections of the CMPPA concerning the protection of the privacy rights of individuals. Treasury's Privacy Act Officer coordinates, reviews, revises, and submits notices as required by the CMPPA, including reporting to Congress and publishing computer matching agreements in the Federal Register on behalf of Treasury. See Table 4 in Appendix D for a list of Treasury computer matching agreements.

INTERAGENCY LEADERSHIP AND COORDINATION

Consumer Financial Protection Bureau (CFPB)

Throughout FY 2011 and FY 2012, OPTR provided subject matter expertise to the newly created CFPB by providing guidance on PIAs, SORNs, and allowing CFPB to use Treasury's privacy training. In sharing its privacy expertise, Treasury had a direct impact on a new agency by ensuring it was able to meet federal privacy requirements until it was able to stand up its own privacy office. In FY 2012, CFPB hired a Chief Privacy Officer and is now operating autonomously.

The Federal Chief Information Officer Council Privacy Committee

The Federal Chief Information Officer Council (CIO Council) serves as the principle interagency forum for improving practices in the design, modernization, use, sharing, and performance of federal agency information resources. Throughout FY 2011 and 2012, OPTR staff supported the work of the CIO Council as members of the CIO Council Privacy Committee (Privacy Committee or Committee), the principal interagency forum dedicated to improving federal agency privacy practices.

DASPTR staff members currently serve on three of the Committee's five subcommittees: Development and Education, Best Practices, and International Privacy.

In FY 2011, Treasury demonstrated its ongoing support of and commitment to the goals of the Development and Education Subcommittee by aiding in the planning and execution of the 2010 Federal Privacy Summit. The DASPTR served as one of two co-chairs making substantial contributions to the event's planning and direction. In addition, OPTR staff provided logistical support and one staff member served as a panelist for a session addressing PII assessments and reduction efforts.

In FY 2011 and 2012, OPTR staff members regularly attended the Committee's Best Practices Subcommittee meetings, the forum for development and promotion of best practices for federal privacy programs and policies. Two members of OPTR actively participated on the Subcommittee's PII Holdings Assessment working group and provided logistical support for its monthly meetings. In addition, OPTR staff participated in meetings of the PIA and SORN working group. In FY 2011 and 2012, the working groups developed templates to assess and notify the public of the government's use of blogs and social media.

In FY 2012, the DASPTR was appointed to serve as a co-chair of the International Privacy Subcommittee. The Subcommittee's principal focus has been on understanding international data privacy standards and developments. It also promotes consistency in the United States' message by coordinating requests for information from foreign governments regarding the United States Government privacy framework.

The Director of National Intelligence's Chief Privacy and Civil Liberties Officer's Privacy and Civil Liberties Focal Points Group

The Director of National Intelligence's (DNI) Chief Privacy and Civil Liberties Officer's Privacy and Civil Liberties Focal Points Group (Focal Points Group) leads the effort to integrate civil liberties and privacy protections into the policies, procedures, programs, and activities of the Intelligence Community (IC). The Focal Points Group solicits interagency comments on proposed privacy and civil liberties guidance for the IC. The DASPTR and OPCL Director are Treasury's representatives on the Focal Points Group.

In FY 2011, the DASPTR and OPCL Director supported the Focal Points Group effort to develop guidance on the IC's use of publicly available information. The guidance provided instruction for when IC elements should consult with agency civil liberties/privacy officers and attorneys. In addition, OPTR staff provided feedback on the Civil Liberties and Privacy Intelligence Community Enterprise Strategy, a document developed by the DNI's Civil Liberties Protection Office for application to all IC elements.

In FY 2012, OPTR staff attended the IC Social Media Summit. The summit was an opportunity to hold a community-level discussion, engage in critical thinking, and explore topics related to the use of social media to support intelligence activities.

Information Sharing and Access Interagency Policy Committee

The Information Sharing and Access Interagency Policy Committee (ISA IPC) is the primary federal interagency body devoted to information sharing policy development for sharing terrorism-related information necessary to preserve national security. The OPCL Director serves as Treasury's representative to the ISA IPC's Privacy and Civil Liberties Subcommittee

In FY 2012, the OPCL Director began serving as the chairperson of the ISA IPC's Privacy and Civil Liberties Subcommittee's Compliance Review Working Group (CRWG). Under his leadership, the CRWG developed a privacy and civil liberties checklist for implementing the ISE Privacy Guidelines. This checklist consisted of a compilation of the privacy and civil liberties requirements and best practices derived from the ISE Privacy Guidelines. Treasury's Office of Intelligence Analysis (OIA) volunteered to conduct a pilot of the checklist to assess whether there were any potential issues with its implementation by an IC element.

LEADERSHIP IN INTERNATIONAL AGREEMENTS AND EVENTS

Terrorist Finance Tracking Program

In FY 2011 and 2012, the DASPTR and OPCL Director participated in the implementation of the "Agreement Between the European Union (EU) and the United States of America on the Processing and Transfer of Financial Messaging Data from the European Union to the United States for the Purposes of the Terrorist Finance Tracking Program" (TFTP Agreement). The TFTP Agreement allows Treasury to use EU-stored data to track terrorism financing while protecting the privacy interests of EU citizens. The DASPTR and OPCL Director have also participated in annual privacy reviews by which EU and U.S. officials review the TFTP program to ensure U.S. compliance under the agreement.

U.S.-EU Data Privacy and Protection in Law Enforcement, Criminal Justice and Public Security Matters

In FY 2011 and 2012, the DASPTR and OPCL Director participated in the negotiations between the United States and the EU on the Data Protection and Privacy Agreement (DPPA). The DPPA negotiations are an effort to establish standard data protection provisions for future personal information sharing for law enforcement purposes between the United States, the EU, and EU member states. The effort will make it easier for the United States and the EU to launch new initiatives to share information for the purpose of more effective law enforcement, while ensuring personal information protection.

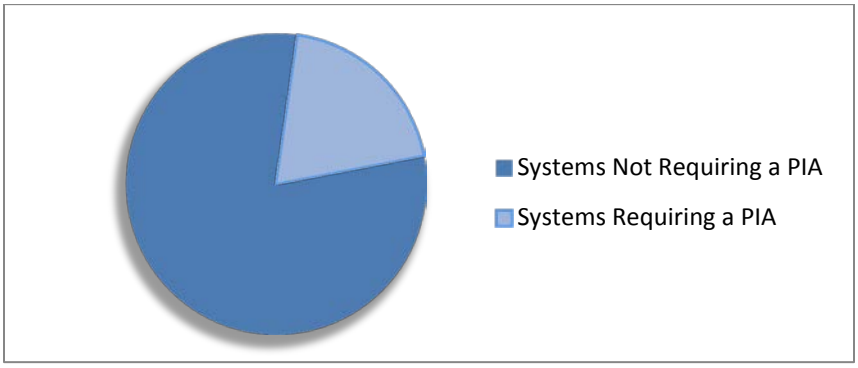
FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002

FISMA requires each agency to develop, document, and implement an agency-wide program to provide security for the information and information systems that support its operations.

FISMA requires agency CIOs, Inspectors General (IG), and SAOPs to report to OMB responses to information security questions that address areas of risk. These questions are designed to assess the implementation of security capabilities and measure their effectiveness. OPTR is responsible for tracking FISMA privacy compliance for Treasury systems and completing the section of the Department's annual report on privacy reporting.

To ensure protections are in place for PII, agencies must report performance metrics related to their privacy management programs. This entails tracking and reporting the number of Treasury systems that contain PII, the number of systems requiring a PIA and/or SORN, and the number of systems that have completed a PIA and/or SORN.

Figure 1: FY 2011 and FY 2012 FISMA Reporting - PIAs



For FY 2011 and 2012, Treasury's inventory of systems experienced slight changes. For FY 2012, the Department reported a total inventory of 305 FISMA systems, all containing personal information in identifiable form. In FY 2011 and 2012, 100 percent of the Treasury systems known to require a PIA or SORN completed the required documentation and publication requirements. Figure 1 shows that during the reporting period, 240 (FY 2011) and 250 (FY 2012) of the 305 systems reported for FISMA required a PIA under Section 208 of the E-Gov Act.

SECTION 803 REPORTING

Pursuant to Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007, CPCLOs must ensure that adequate processes exist to receive, investigate, respond to, and redress complaints from individuals who allege privacy or civil liberties violations. To meet the requirement, the Department issued 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,* which directs heads of bureaus and relevant offices to establish internal procedures to ensure accurate and complete reporting to OPTR.

Each quarter, OPTR issues a data call to prepare for 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 CPCLO.

The ASM continues to provide timely submissions of the Section 803 metrics to Congress on behalf of the Department. For FY 2011 and 2012, the Department performed 1,073 and 741 reviews respectively, provided advice and responses 56 times in 2011 and 12 times in 2012, and responded to no privacy and civil liberties complaints in 2011 and two in 2012. The types of reviews the Department and its bureaus conducted included:

Types of Reviews	FY 2011	FY2012
Privacy Threshold Assessments/Privacy Impact Assessments	162	206
System of Records Notices and Routine Uses	83	139
Exhibit 300 Process	416	167
5 CFR 1320 (PRA/Information Collection Request)	220	148
Social Security Number Redaction/Elimination	45	69
Computer Matching Agreement Program	44	2
Records Management/Other Types	103	10

PRIVACY AND CIVIL LIBERTIES PROTECTION GOALS FOR 2013

In FY 2013, OPTR will coordinate within Treasury to achieve the following privacy and civil liberties goals:

- Finalize TD 25-10, *Information Sharing Environment Privacy and Civil Liberties Policy*;
- Assist bureaus involved in the ISE with identifying personnel who need to be trained on the implementation of TD 25-10;
- Work with appropriate bureaus and offices to develop ISE training as part of the implementation of TD 25-10;
- Collaborate with OGC, the OCIO and the Office of Public Affairs to complete Treasury's social media policy;
- Ensure that all bureaus with a social media presence complete a PIA;
- Work with bureaus and Departmental Offices to ensure they update their information in the PII Holdings Database;
- Participate in Treasury and inter-agency working groups to provide sound privacy subject matter expertise for the implementation of Executive Order 13636 and Presidential Policy Directive 21; and
- Reduce the number of unencrypted PII losses.

APPENDIX A: LIST OF ACRONYMS

ASM	Assistant Secretary for Management
CFPB	Consumer Financial Protection Bureau
CIO	Chief Information Officer
CPCLO	Chief Privacy and Civil Liberties Officer
CPO	Chief Privacy Officer
DASPTR	Deputy Assistant Secretary Privacy, Transparency, and Records
DIB	Data Integrity Board
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
IG	Inspector General
IIF	Information in Identifiable Form
IRS	Internal Revenue Service
ISE	Information Sharing Environment
IT	Information Technology
NIST	National Institute of Standards and Technology
OCC	Office of the Comptroller of the Currency
OCIO	Office of the Chief Information Officer
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
SAOP	Senior Agency Official for Privacy
SORN	System of Records Notice
TCSIRC	Treasury Computer Security Information Response Center
TD	Treasury Directive
TIGTA	Treasury Inspector General for Tax Administration

APPENDIX B: LIST OF KEY LAWS, REGULATIONS, AND OMB POLICIES APPLICABLE TO TREASURY DEPARTMENT PRIVACY ACTIVITIES

Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6506, imposes restrictions on websites that are collecting information from children under the age of thirteen in order to protect children's privacy and safety online. By policy, federal websites must adhere to the Act's requirements.

Clinger-Cohen Act of 1996, Pub. L. No. 104-106, Div. E, requires government information technology to operate 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 OCIO.

Consolidated Appropriations Act of 2005 § 522, Pub. L. No. 108-447, requires specific agencies to submit an annual report to Congress on Department activities that affect privacy.

E-Government Act of 2002 § 208, Pub. L. No. 107-347, requires, among many other things, an annual report to Congress describing efforts at accomplishing E-Gov initiatives, to include capital planning and an executive summary highlighting significant issues.

Federal Information Security Management Act of 2002, Pub. L. No. 107-347, requires 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.

Freedom of Information Act, as amended, 5 U.S.C. § 552, provides for the disclosure of information maintained by federal agencies to the public while allowing limited protections for privacy.

Implementing the Recommendations of the 9/11 Commission Act of 2007 § 803, Pub. L. No. 110-53, requires agencies to appoint a senior officer as the PCLO.

Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) § 1016(d), Pub. L. No. 108-458, requires guidelines for protecting privacy and civil liberties in the context of the ISE.

Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes privacy protections, including systems of records notices to notify the public of records the federal government maintains.

31 C.F.R. pt. 1, Disclosure of Records

Executive Order 13388, "Further Strengthening the Sharing of Terrorism Information to Protect Americans," establishes the requirement that ISE communities create IT and privacy guidelines for sharing terrorist information.

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, "Instructions on 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"
OMB Memo, "Recommendations for Identity Theft Related Data Breach Notification" (Sept. 20, 2006)
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"
OMB M-10-22, "Guidance for Online Use of Web Measurement and Customization Technologies"
OMB M-10-23, "Guidance for Agency Use of Third-Party Websites and Applications"

APPENDIX C: DEPARTMENT OF TREASURY BUREAUS AND OFFICES

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

APPENDIX D: REFERENCE TABLES

FY 2011 Published SORNs

Title	Date	Published
Privacy Act Compilation		
BPD Systems of Records – Compilation	8/17/11	76 FR 51128
New/Altered Privacy Act Notices Published		
Alteration: OCC .210 – Bank Securities Dealers System	9/13/11	76 FR 56501
Alteration: OCC .220 – Section 914 Tracking System	9/13/11	76 FR 56501
Alteration: OCC .600 – Consumer Complaint and Inquiry System	9/13/11	76 FR 56501
Treasury .013 – Department of the Treasury Civil Rights Complaints and Compliance Review Files	9/8/11	76 FR 55737
Alteration: FMS .008 – Mailing List Records	8/17/11	76 FR 51123
Alteration: DO .191 – Human Resources and Administrative Records System	7/28/11	76 FR 45336
Alteration: FMS .006 – Direct Deposit Enrollment Records	7/19/11	76 FR 42765
DO .226 – Validating EITC Eligibility with State Data Pilot Project Records	7/7/11	76 FR 39980
Alteration: DO .218 – Home Affordable Modification Program Records	6/24/11	76 FR 37193
Alteration: Treasury .004 – FOIA/PA Request Records	4/29/11	76 FR 24085
IRS 42.888 – Qualifying Therapeutic Discovery Project Records	3/31/11	76 FR 17997
DO .225 – TARP Fraud Investigation Information System	2/9/11	76 FR 7239

Title	Date	Published
OTS .013 – Mass Communication System	2/9/11	76 FR 7242
OTS .015 – Retiree Billing System	2/9/11	76 FR 7243
Alteration: DO .120 – Records Related to Office of Foreign Assets Control Economic Sanctions	1/27/11	76 FR 4995
FMS .008 – Mailing List Records	12/16/10	75 FR 78802
Alteration: IRS/OPR IRS 37.006, Correspondence, Miscellaneous Records, and Information Management Records; 37.007, Practitioner Disciplinary Records; and 37.009, Enrolled Agents and Resigned Enrolled Agents	10/19/10	75 FR 64403
Alteration: DO .120 – Records Related to Office of Foreign Assets Control Economic Sanctions	10/6/10	75 FR 61853

FY 2011 Published Consumer Financial Protection Bureau SORNs

Title	Date	Published
DO .321 – CFPB Implementation Team External Affairs Database	7/7/11	76 FR 39978
DO .318 – CFPB Implementation Team Correspondence Tracking	6/15/11	76 FR 35071
DO .316 – CFPB Implementation Team Benefits and Retirement Systems	2/15/11	76 FR 8843
DO .315 – CFPB Implementation Team Consumer Inquiry	1/10/11	76 FR 1507
DO .320 – CFPB Implementation Team Mailing Lists Databases	12/30/10	75 FR 82427

FY 2011 Treasury Computer Matching Agreement

Matching Agreement	Date	Published
IRS Disclosure of Information to Federal, State and Local Agencies (DIFSLA) Computer Matching Program	5/2/11	76 FR 24564

FY 2012 Treasury, SORNs, Compilations, and Computer Matching Agreements

FinCEN Systems of Records - Compilation	10/1/12	77 FR 60014
IRS Systems of Records - Compilation	8/10/12	77 FR 47930
TTB System of Records - Compilation	12/1/11	76 FR 74847
OCC Systems of Records - Compilation	4/3/12	77 FR 20104
31 CFR 1.36, as Amended	5/15/12	77 FR 28478
IRS 37 .007 Practitioner Disciplinary Records - Alteration	9/14/12	77 FR 56913
DO .218 Making Home Affordable Program - Revised Notice	4/2/12	77 FR 19751
DO .196 Security Information System - Revised Notice	2/15/12	77 FR 8954
FMS .002 Payment Issue Records for Regular Recurring Benefit Payments – Revised and consolidated notices	2/15/12	77 FR 8947
FMS .016 Payment Records for Other Than Regular Recurring Benefit Payments - Revised and consolidated notices	2/15/12	77 FR 8947
FMS .014 Debt Collection Operations System - Revised and consolidated notices	2/15/12	77 FR 8947
BEP .021 Investigative Files- Revised notice	1/6/12	77 FR 8377
BEP .027 Access Control and Alarm Monitoring Systems (ACAMS) -	1/5/12	77 FR 551

Revised notice		
IRS 37.111 Preparer Tax Identification Number Records (TIN) - New notice	11/15/11	76 FR 70813
IRS Notice of Proposed Alterations to consolidate 12 Privacy Act Systems of Records	11/15/12	76 FR 70815
Final Rules		
Treasury Office of Civil Rights and Diversity System of Records - Final rule	1/11/12	77 FR 1632
Treasury/IRS 37.111- Preparer Tax Identification Number Records System of Records Final rule	11/17/11	76 FR 71293
IRS Consolidation of 12 System of Records - Final rule	11/5/11	76 FR 70640
CMA Notices		
Notice of Treasury Internal Revenue Service Data Loss Prevention Project Computer Matching Program	3/21/13	78 FR 17471
Notice of a Treasury Inspector General for Tax Administration/Internal Revenue Service Computer Matching Program	3/6/12	77 FR 13388