



# Audit Report



## AUDIT REPORT

INFORMATION TECHNOLOGY: United States Department of the Treasury's Compliance with Section 522 of the Consolidated Appropriations Act of 2005 (OIG-09-014)

December 3, 2008

## Office of Inspector General

Department of the Treasury



OFFICE OF  
INSPECTOR GENERAL

DEPARTMENT OF THE TREASURY  
WASHINGTON, D.C. 20220

December 3, 2008

**MEMORANDUM FOR PETER B. MCCARTHY  
ASSISTANT SECRETARY FOR MANAGEMENT AND  
CHIEF FINANCIAL OFFICER**

**ELIZABETH CUFFE  
DEPUTY ASSISTANT SECRETARY FOR PRIVACY AND  
TREASURY RECORDS**

**FROM:** Joel Grover /s/  
Deputy Assistant Inspector General for Financial Management  
and IT Audits

**SUBJECT:** Audit Report – United States Department of the Treasury’s  
Compliance with Section 522 of the Consolidated  
Appropriations Act of 2005

The attached report presents the results of our audit of the United States Department of the Treasury’s (Treasury) compliance with Section 522 of the Consolidated Appropriations Act of 2005, as amended (Section 522) and Office of Management and Budget (OMB) Memorandum 07-16 (M-07-016), *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*. To meet the Section 522 requirement for a periodic Inspector General audit of the agency’s privacy program, we contracted with KPMG LLP, an independent certified public accounting firm. This audit includes the Treasury and its bureaus with the exception of the Internal Revenue Service (IRS). The Treasury Inspector General for Tax Administration (TIGTA) performed an assessment of M-07-016 compliance at the IRS as part of its annual FISMA evaluation<sup>1</sup>.

Based on the results reported by KPMG, we determined that Treasury did not fully comply with Section 522 and did not comply with M-07-016. Specifically, KPMG reported that (1) annual congressional reporting requirements were not met, (2)

---

<sup>1</sup> TIGTA’s annual IRS FISMA evaluation results (Audit #200820024) were included as Attachment 2 to the OIG report *INFORMATION TECHNOLOGY: Federal Information Security Management Act Fiscal Year 2008 Performance Audit* (OIG-08-046) dated September 26, 2008

Page 2

reporting requirements to the OIG were not met, and (3) policies and procedures required by Section 522 and OMB Memorandum 07-16 were still in draft.

If you have questions or require further information, you may contact me at (202) 927-5768, or Tram Dang at (202) 927-5171.

Attachment

## **ATTACHMENT**

United States Department of the Treasury's  
Compliance with Section 522 of the  
Consolidated Appropriations Act of 2005  
December 2, 2008

*United States Department of the Treasury's  
Compliance with Section 522 of the Consolidated  
Appropriations Act of 2005*

Prepared for the United States Department of the Treasury  
Office of the Inspector General

Prepared by KPMG LLP

December 2, 2008

**TABLE OF CONTENTS**

EXECUTIVE SUMMARY ..... 1  
BACKGROUND ..... 4  
OBJECTIVE, SCOPE, AND METHODOLOGY ..... 7  
RESULTS ..... 9  
CONCLUSION..... 11  
MANAGEMENT RESPONSE TO REPORT ..... 12  
APPENDIX I – ACRONYM LIST..... I-1



KPMG LLP  
2001 M Street, NW  
Washington, DC 20036

## EXECUTIVE SUMMARY

December 2, 2008

Joel Grover

Deputy Assistant Inspector General for Financial Management and Information Technology Audits

United States Department of the Treasury

740 15th Street NW, Suite 600

Washington, DC 20220

Dear Mr. Grover:

This report presents the results of our audit of the United States Department of the Treasury's (Treasury) non-Internal Revenue Service (IRS) privacy data protection program and practices, as required by Section 522 of the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005, Public Law 108-447, as amended, (hereinafter referred to as Section 522). Section 522 requires the following:

1. Appoint a Chief Privacy Officer (CPO) to assume primary responsibility for privacy and data protection policy.
2. Establish privacy and data protection procedures and policies.
3. Prepare a written report of the use of information in an identifiable form (IIF) and privacy and data protection procedures to be recorded with the Inspector General (IG) to serve as a benchmark for the agency.
4. Perform an independent, third-party review of the use of IIF.

Additionally, Section 522 requires that the agency's IG perform a periodic assessment of the implementation of this section. The agency IG shall report the results to the Committee on Appropriations of the House and Senate, the House Committee on Oversight and Government Reform, and the Senate Committee on Homeland Security and Government Affairs<sup>1</sup>.

Agencies were required to be compliant with Section 522 by December 8, 2005.

The Treasury Office of the Inspector General (OIG) contracted with KPMG LLP (KPMG) to conduct a performance audit of the Treasury's privacy program pursuant to Section 522 and Office of Management and Budget (OMB) Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*. We conducted this performance audit in accordance with the standards applicable to such audits contained in Generally Accepted Government Auditing Standards (GAGAS), issued by the Comptroller General of the United States. These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The objective of our performance audit was to determine the effectiveness of Treasury's privacy and data protection programs and practices in complying with Section 522 and OMB Memorandum 07-16. The

---

<sup>1</sup> As amended in Section 742 of the Consolidated Appropriations Act, 2008, Public Law 110-161.



scope of our performance audit included reviewing program effectiveness from both a (1) top-down department-level perspective to assess overall program management capabilities in developing and implementing privacy requirements to be carried out by bureaus, and (2) bottom-up non-IRS Treasury bureau-level perspective to assess the effectiveness of privacy programs implemented by bureaus for Treasury-specific functions and applications.

During our performance audit to determine compliance with Section 522 and OMB Memorandum 07-16, we determined that Treasury did not fully comply with Section 522 and did not comply with OMB Memorandum 07-16. Specifically, we found that (1) annual congressional reporting requirements were not met, (2) reporting requirements to the OIG were not met, and (3) policies and procedures required by Section 522 and OMB Memorandum 07-16 were still in draft. Treasury should ensure that its privacy and data protection program and practices comply with Section 522 and OMB Memorandum 07-16. Specific areas include:

- 1. Annual Congressional Reporting Requirements Were Not Met.** The Treasury has not prepared and submitted an annual report to Congress on activities that affect privacy, including complaints of privacy violations, implementation of Section 522a of Title 5, 11 United States Code, internal controls, and other relevant matters.
- 2. Reporting Requirements to the OIG Were Not Met.** The Treasury did not record with the OIG a written report on the use of IIF, as well as its privacy and data protection policies and procedures.
- 3. Policies and Procedures Required by Section 522 and OMB Memorandum 07-16 Were in Draft.** Two (2) Treasury directives and policies related to the collection, use, sharing, disclosure, transfer, and storage of personally identifiable information (PII) were still in draft.

While several of Treasury's policies and procedures required by Section 522 and OMB Memorandum 07-16 were in draft at the conclusion of fieldwork, the majority of non-IRS bureaus have begun to adopt them<sup>2</sup>. Specifically, each of the 12 non-IRS bureaus had begun performing privacy impact assessments (PIAs) on information systems. In addition, bureaus have begun to provide training on the responsibilities of individuals authorized to access PII. Lastly, through our limited procedures, we noted that Treasury is adequately protecting PII on public Internet sites, intranet sites, and general support systems<sup>3</sup>.

Overall, we determined that Treasury did not fully comply with Section 522 and did not comply with OMB Memorandum 07-16. We are reporting exceptions with the extent policies and reporting requirements required by Section 522 and OMB Memorandum 07-16 were not finalized. All of our findings are included in the results section of this report, which warrants management attention and corrective action.

This performance audit did not constitute an audit of financial statements in accordance with *Government Auditing Standards*. KPMG was not engaged to, and did not, render an opinion on Treasury's internal controls over financial reporting or over financial management systems (for purposes of OMB Circular Number. A-127, *Financial Management Systems*, July 23, 1993, as revised). KPMG cautions that

---

<sup>2</sup> An assessment of the IRS's compliance with the provisions of Section 522 and OMB Memorandum 07-16 was performed by Treasury Inspector General for Tax Administration (TIGTA) as part of its annual independent Federal Information Security Management Act evaluation. See Department of the Treasury – OIG Audit Report OIG-08-046 – Attachment 2.

<sup>3</sup> Our limited procedures included manual inspections of the all Treasury publicly available Internet Web sites, four (4) judgmentally selected intranets, and one (1) judgmentally selected general support system.





projecting the results of our evaluation to future periods is subject to the risk that controls may become inadequate because of changes in conditions or because compliance with controls may deteriorate.

Sincerely,

KPMG LLP

## BACKGROUND

Enacted in December 2004, Section 522 directs agencies, including Treasury, to implement a number of measures to protect IIF. Such measures require that agencies:

1. Appoint a CPO to assume primary responsibility for agency privacy and data protection policy. Specifically, Section 522 requires that the CPO:
  - a. Assure that the use of technologies sustain, and do not erode, privacy protection related to the use, collection, and disclosure of IIF;
  - b. Assure that technologies used to collect, use, store, and disclose IIF 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;
  - c. Assure 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;
  - d. Evaluate legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government;
  - e. Conduct a privacy impact assessment of proposed rules of the Department on the privacy of IIF, including the type of PII collected and the number of people affected;
  - f. Prepare 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;
  - g. Ensure that the Department protects information in an identifiable form and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction;
  - h. Train and educate employees on privacy and data protection policies to promote awareness of and compliance with established privacy and data protection policies;
  - i. Ensure compliance with the Departments established privacy and data protection policies.
2. Establish and implement comprehensive privacy and data protection procedures governing the collection, use, sharing, disclosure, transfer, storage, and security of IIF relating to agency employees and the public. Such procedures are to be consistent with legal and regulatory guidance, including OMB regulations, the Privacy Act of 1974, and section 208 of the E-Government Act of 2002.
3. Perform an independent, third party review of the use of IIF.
4. Prepare a written report, signed by the CPO that provides a benchmark for the agency's privacy program and describes the agency's use of IIF, along with its privacy and data protection policies and procedures. The report is to be recorded with the agency IG.
5. The agency's IG perform a periodic assessment of the implementation of Section 522. Section 522 further requires that the agency IG shall report the results to the Committee on Appropriations of the

House and Senate, the House Committee on Oversight and Government Reform, and the Senate Committee on Homeland Security and Government Affairs<sup>4</sup>.

OMB issued Memorandum 07-16 on May 22, 2007, which requires agencies to develop and implement notification policies for the breach of PII. Agencies were required to implement these breach notification policies by September 22, 2007. OMB Memorandum 07-16 required that the policies include existing and new requirements for internal incident handling and reporting, external breach notification, and the development of policies regarding the responsibilities of individuals authorized to access PII.

### **Treasury Mission and Organization**

The Treasury operates and maintains systems that collect, process, store, and distribute mission-critical information, such as taxpayer and bank data, in support of Treasury functions critical to the nation's financial infrastructure. These functions included the production of coin and currency, the disbursement of payments to the American public, revenue collection, and the borrowing of funds necessary to run the Federal Government. Management and performance accountability of these functions and systems are overseen by the Treasury's 13 operating bureaus and offices, including:

- **Alcohol and Tobacco Tax and Trade Bureau** – Responsible for enforcing and administering laws covering the production, use, and distribution of alcohol and tobacco products. The Alcohol and Tobacco Tax and Trade Bureau also collects excise taxes for firearms and ammunition.
- **Bureau of Engraving and Printing** – Designs and manufactures U.S. (paper) currency, many stamps, securities, and other official certificates and awards.
- **Bureau of the Public Debt** – Borrows the money needed to operate the Federal Government. It administers the public debt by issuing and servicing U.S. Treasury marketable, savings, and special securities.
- **Community Development Financial Institution Fund** – Created to expand the availability of credit, investment capital, and financial services in distressed urban and rural communities.
- **Departmental Offices** – Primarily responsible for policy formulation. The Departmental Offices are composed of divisions headed by Assistant Secretaries, some of whom report to Under Secretaries.
- **Financial Crimes Enforcement Network** – Supports law enforcement investigative efforts and fosters interagency and global cooperation against domestic and international financial crimes. It also provides U.S. policy makers with strategic analyses of domestic and worldwide trends and patterns.
- **Financial Management Service** – Receives and disburses all public monies, maintains government accounts, and prepares daily and monthly reports on the status of government finances.
- **IRS** – Responsible for determining, assessing, and collecting internal revenue in the United States.
- **Office of the Comptroller of the Currency** – Charters, regulates, and supervises national banks to ensure a safe, sound, and competitive banking system that supports the citizens, communities, and economy of the United States.
- **OIG** – Conducts and supervises audits and investigations of Treasury programs and operations. The OIG also keeps the Secretary and the Congress fully and currently informed about problems, abuses, and deficiencies in Treasury programs and operations.
- **Office of Thrift Supervision** – The primary regulator of all Federal and many state-chartered thrift institutions, which include savings banks and savings and loan associations.
- **United States Mint** – Designs and manufactures domestic, bullion, and foreign coins as well as commemorative medals and other numismatic items. The Mint also distributes United States coins to the Federal Reserve banks as well as maintains physical custody and protection of our nation's silver and gold assets.

---

<sup>4</sup> As amended in Section 742 of the Consolidated Appropriations Act, 2008, Public Law 110-161.

- **TIGTA** – Conducts and supervises audits and investigations of IRS programs and operations. The TIGTA also keeps the Secretary and the Congress fully and currently informed about problems, abuses, and deficiencies in IRS programs and operations.

### **Treasury Privacy and Data Protection Program**

Treasury established a department wide privacy program to protect the PII it manages from unauthorized use, access, disclosure, or sharing and to safeguard associated information systems from unauthorized access, modification, disruption, or destruction. Key components of the Treasury's privacy program include, but are not limited to, the:

- Assistant Secretary for Management/Chief Financial Officer designated as the CPO and Senior Agency Official for Privacy with overall responsibilities for the program in March of 2005.
- Office of Privacy and Treasury Records (OPTR) was established on March 24, 2008 as the program management office that supports the Treasury CPO in developing and implementing privacy requirements including policies and procedures for managing and protecting PII. OPTR also provides privacy and data protection programs oversight of all Treasury bureaus and offices in carrying out directives and policies developed by OPTR. Additionally, OPTR is responsible for establishing a privacy awareness program disseminated to bureaus regarding Treasury employee privacy responsibilities. Prior to this date, the Office of the Chief Information Officer (OCIO) held these responsibilities. OPTR includes the Office of Privacy and Civil Liberties, Office of Disclosure Services, Treasury Records, Treasury Library, and the Orders and Directives Program.
- Each of the 13 Treasury bureaus has also established a bureau privacy officer<sup>5</sup>. The role of the bureau privacy officer is to act as a liaison between the bureau's system owners and the OPTR and the CPO to ensure that privacy and data protection programs are operating effectively at the bureau level. This includes performance of Privacy Threshold Analysis and PIAs on all information systems. Bureau privacy officers work with the system owners to analyze the data being processed in the system and make a determination if the data contains PII.

---

<sup>5</sup> This report excludes privacy and data protection programs at IRS.

## **OBJECTIVE, SCOPE, AND METHODOLOGY**

The objective of the audit was to determine the effectiveness of Treasury's privacy and data protection programs and practices in complying with Section 522 and OMB Memorandum 07-16. The scope of our audit included reviewing program effectiveness from both a (1) top-down department level perspective to assess overall program management capabilities in developing and implementing privacy requirements to be carried out by bureaus, and (2) bottom-up non-IRS Treasury bureau-level perspective to assess the effectiveness of privacy programs implemented by bureaus for Treasury-specific functions and applications.

To accomplish our objectives, KPMG conducted interviews with appropriate Treasury officials from OPTR and bureau-level officials to obtain an understanding of each area within the scope of the audit. Further, we reviewed Treasury policy, directives, and guidelines relative to privacy and data protection, selected documentation applicable to bureau-level activities performed including PIAs, and performed procedures to identify the presence of PII on publicly accessible Internet sites, internal intranet sites, and one (1) general support system.

### **Top-down Department Level Review**

To determine Treasury effectiveness in establishing a privacy program for implementing privacy requirements, KPMG reviewed privacy program management capabilities established to support the Treasury CPO in developing and implementing privacy requirements. This included reviewing policies directives and procedures for managing and protecting PII, a process for identifying PII in applications, and procedures for conducting PIAs of applications and systems containing PII. KPMG also reviewed roles, responsibilities, and the effectiveness of oversight capabilities at the department level in managing and directing the privacy program activities performed by Treasury bureaus, and development of a privacy awareness program.

### **Bottom-up Bureau Level Review**

To determine effectiveness of privacy requirements carried out by Treasury bureaus from departmental direction provided, KPMG reviewed privacy activities performed by non-IRS Treasury bureaus for specific functions and applications, through a representative subset of 23 information systems. Our review included an assessment of the effectiveness of privacy threshold analysis and PIAs performed on information systems in analyzing systems for PII. Our test work also included limited procedures to determine the presence of PII on the Treasury publicly accessible Internet, intranet, and on one (1) general support system.

### **Other Considerations**

KPMG performed this performance audit at Treasury's headquarters offices in Washington, DC and bureau locations in Washington, DC, Hyattsville, MD, McLean, VA, and Parkersburg, WV during the period of May through September 2008. Throughout the audit, we met with Treasury management to discuss our preliminary conclusions.

The Treasury OIG contracted with KPMG to audit Treasury's compliance with Section 522 and OMB Memorandum 07-16, and report on the effectiveness of Treasury's privacy and data protection program. KPMG conducted this performance audit in accordance with GAGAS issued by the Comptroller General of the United States. These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit

objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

### **Applicable Criteria**

KPMG's criteria for this performance audit are based on Federal privacy and data protection criteria established by Law and OMB.

- Section 522, Division H of the Consolidated Appropriations Act, 2005
- OMB Memorandum 08-21, *FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*
- OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*

## RESULTS

During our performance audit to determine compliance with Section 522 and OMB Memorandum 07-16, we determined that Treasury did not fully comply with Section 522 and did not comply with OMB Memorandum 07-16. Specifically, we found that (1) annual congressional reporting requirements were not met, (2) reporting requirements to the OIG were not met, and (3) policies and procedures required by Section 522 and OMB Memorandum 07-16 were not finalized. Treasury should ensure that its privacy and data protection program and practices fully comply with applicable Congressional and OMB requirements.

## FINDINGS

### 1. Annual Congressional Reporting Requirements Have Not Been Met.

Treasury has not prepared and submitted any annual reports to Congress on activities 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.

According to OPTR management, from December 8, 2004 to March 23, 2008, the OCIO held the responsibility for privacy and data protection, but due to limited resources the OCIO did not prepare and submit the annual report to Congress on activities affecting privacy. Since March 24, 2008, OPTR had the responsibility to develop the annual report to Congress on activities affecting privacy, but due to competing priorities, the annual reports have not been prepared and submitted.

By not submitting the report on an annual basis, Treasury is not in compliance with Section 522, and Congress may not be aware of the current state of the agency's privacy-related activities. This could result in the inability to dedicate adequate resources to the protection of IIF.

We recommend that OPTR management:

1. Prepare a report to Congress on an annual basis on activities of the Treasury 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.

### 2. Reporting Requirements to the OIG Were Not Met.

Treasury did not record with the OIG a written report on the use of IIF, as well as its privacy and data protection policies and procedures.

According to OPTR management, from December 8, 2004 to March 23, 2008, the OCIO held the responsibility for privacy and data protection, but due to limited resources the OCIO did not prepare and submit the report to the OIG on the use of IIF. Since March 24, 2008, OPTR had the responsibility to submit the report to the OIG on the use of IIF, but due to competing priorities, the reports have not been prepared and submitted.

By not recording a report on the use of IIF, as well as the privacy and data protection policies and procedures with the OIG, the Treasury is not in compliance with Section 522. Furthermore, Treasury does not have a benchmark on its use of IIF, along with privacy and data protection policies and procedures.

We recommend that OPTR management:

2. Record a formal written report on the use of IIF, as well as privacy and data protection policies and procedures with the OIG.

### **3. Policies and Procedures Required by Section 522 and OMB Memorandum 07-16 Are in Draft**

Section 522 of the Consolidated Appropriations Act, 2005, issued on December 8, 2004, required agencies to develop policies and procedures for privacy and data protection within one (1) year of the law being signed. In addition, OMB Memorandum 07-16, issued on May 22, 2007, required that policies be developed for the PII breach notifications. OMB Memorandum 07-16 required that these policies and procedures be issued within 120 days after the date of the memorandum, September 22, 2007. To date, Treasury has only finalized Treasury Directive (TD) 25-07 *Privacy Impact Assessment*, dated August 6, 2008, and TD 25-09 *Privacy and Civil Liberties Activities Pursuant to Section 803 of The Implementing Recommendation of the 9/11 Commission Act of 2007, P.L. 110.53*, dated September 3, 2008. However, Treasury Directive Publication 25-07 *Privacy Impact Assessment Manual* and TD 25-08 *Personally Identifiable Information (PII) Protection, Breach Response, and Notification* are still in draft.

According to OPTR management, from December 8, 2004 to March 23, 2008, the OCIO held the responsibility for privacy and data protection functions under Section 522. The OCIO had developed directives and policies in accordance with Section 522 and OMB Memorandum 07-16; however, the clearance process was delayed citing limited resources to complete the process and pending the creation of OPTR. Since its creation on March 24, 2008, OPTR has assumed the responsibility to review and update the content of these directives and policies and continue the formal clearance process.

Without formal directives and policies related to the collection, use, sharing, disclosure, transfer, and storage of PII in place at the Treasury, IIF may not be adequately protected. However, the majority of non-IRS bureaus have begun to adopt all draft policies and procedures. Specifically, each of the 12 non-IRS bureaus had begun performing PIAs on information systems. In addition, bureaus have begun to provide training on the responsibilities of individuals authorized to access PII. Lastly, through our limited procedures, we noted that Treasury is adequately protecting PII on public Internet sites, intranet sites, and general support systems.

We recommend that OPTR management:

3. Finalize all of the directives and policies related to the collection, use, sharing, disclosure, transfer, and storage of PII identified above.



## **CONCLUSION**

We assessed Treasury for compliance with Section 522 and OMB Memorandum 07-16. Overall, we determined that Treasury did not fully comply with Section 522 and did not comply with OMB Memorandum 07-16. We are reporting exceptions with the extent policies, and reporting requirements required by Section 522 and OMB Memorandum 07-16 were not implemented. All of our findings are included in the results section of this report, which warrants management attention and corrective action.

# MANAGEMENT RESPONSE TO REPORT




ASSISTANT SECRETARY

DEPARTMENT OF THE TREASURY  
WASHINGTON, D.C.

NOV 21 2008

**MEMORANDUM FOR JOEL GROVER  
DEPUTY ASSISTANT INSPECTOR GENERAL FOR  
FINANCIAL MANAGEMENT AND IT AUDITS**

**FROM:** Peter B. McCarthy  
Assistant Secretary for Management  
and Chief Financial Officer 

**SUBJECT:** Response to Draft Audit Report – INFORMATION  
TECHNOLOGY: U.S. Department of the Treasury's  
Compliance with Section 522 of the Consolidated  
Appropriations Act of 2005

Thank you for the opportunity to review and comment on the subject draft report. The draft report states that the Treasury Department is not compliant with three specific parts of Section 522 of the Consolidated Appropriations Act of 2005. We have reviewed the details of the report and concur with the three findings.

The Office of Privacy and Treasury Records was established in March 2008 in order to consolidate information privacy functions and to elevate the privacy office to directly report to the Assistant Secretary for Management and Chief Financial Officer, who is the Senior Agency Official for Privacy. The objectives of this realignment were to ensure that all information privacy functions were combined under one line of authority and to create conditions for a sustainable, Treasury-wide information privacy program. We are committed to continuing to strengthen the Treasury information privacy program and to addressing the Section 522 requirements.

Should you have any questions pertaining to this response, please do not hesitate to contact me or Libby Cuffe, Deputy Assistant Secretary for Privacy and Treasury Records, at 622-1682 or [Elizabeth.Cuffe@do.treas.gov](mailto:Elizabeth.Cuffe@do.treas.gov).

## APPENDIX I – ACRONYM LIST

<b>Acronym</b>	<b>Definition</b>
<b>CPO</b>	Chief Privacy Officer
<b>GAGAS</b>	Generally Accepted Government Auditing Standards
<b>IG</b>	Inspector General
<b>IIF</b>	Information in an Identifiable Form
<b>IRS</b>	Internal Revenue Service
<b>KPMG</b>	KPMG LLP
<b>OCIO</b>	Office of the Chief Information Officer
<b>OMB</b>	Office of Management and Budget
<b>OIG</b>	Office of the Inspector General
<b>OPTR</b>	Office of Privacy and Treasury Records
<b>PIA</b>	Privacy Impact Assessment
<b>PII</b>	Personally Identifiable Information
<b>TD</b>	Treasury Directive
<b>TIGTA</b>	Treasury Inspector General for Tax Administration
<b>Treasury</b>	United States Department of the Treasury