Semiannual Report To The Congress

April 1, 2006 – September 30, 2006

Office of Inspector General

DEPARTMENT OF THE TREASURY

HIGHLIGHTS IN BRIEF

During this semiannual reporting period, our **Office of Audit** issued 17 reports and other products which identified, in total, $5.5 million in monetary benefits. Work by our **Office of Investigations** resulted in 14 convictions (12 by plea agreement), 1 federal indictment, 1 federal information, and 15 referrals accepted for prosecution. Investigative activities also resulted in $183,500 in court-ordered fines, restitution, and civil settlements, as well as 10 personnel actions. Some of our significant results for this period are described below:

- We completed four audits related to Treasury's anti-money laundering/terrorist financing and foreign sanctions programs. One audit found that the Office of the Comptroller of the Currency (OCC) took a questionable (non-public) enforcement action against Wells Fargo Bank, the nation's fifth largest bank, when it found serious recurring Bank Secrecy Act (BSA) program deficiencies. Another audit found that the Financial Crimes Enforcement Network was slow in developing possible new leads for law enforcement through analysis of BSA data, devoting most of its analytical work to processing routine data requests. Audits of OCC and the Office of Thrift Supervision found that sampled examinations of financial institutions for compliance with Office of Foreign Assets Control requirements were not documented well enough to determine whether or not the examined institutions were in compliance.

- Our fiscal year 2006 evaluation of Treasury's information security program and practices disclosed deficiencies that, in the aggregate, constituted substantial noncompliance with the Federal Information Security Management Act of 2002. Deficiencies were noted in the areas of certification and accreditation, training, plans of actions and milestones, and incident response processing among others. We also reported several matters pertaining to Treasury's national security systems. We found, however, that the Department was able, for the first time, to develop a systems inventory that is substantially complete and conforms to applicable requirements.

- In August 2006, an individual pled guilty in federal court to a three-count information charging bank fraud, mail fraud, and money laundering from September to December 2005, in a scheme to defraud the Federal Emergency Management Agency (FEMA) of more than $100,000 in relief funds intended for victims of Hurricanes Katrina and Rita. In another case, Treasury OIG led the investigation of an individual for making a false statement on a FEMA application. The individual, a District of Columbia resident, falsely claimed his home was damaged by Hurricane Katrina and received three Treasury checks totaling $14,749. In June 2006, the individual pled guilty in federal court.

- After BEP notified our office that a number of incomplete $100 notes had entered into commerce, OIG special agents, with the assistance of BEP investigators and the U.S. Secret Service, initiated an investigation which the Federal Bureau of Investigations (FBI) later joined. The investigation led to the arrest by OIG and FBI special agents of a BEP employee after the execution of a search warrant at his home recovered partially printed $100 notes stolen from BEP's Eastern Currency Facility in Washington, D.C. On September 6, 2006, pursuant to a plea agreement, he pled guilty to one charge of possession of tools and materials for counterfeiting purposes and is awaiting sentencing.

Finally, we are pleased to report that the work of our office during fiscal year 2006 was recognized with 5 Awards for Excellence by the President's Council on Integrity and Efficiency at an October 2006 ceremony.

A Message From The Inspector General

I am pleased to present the Department of the Treasury (Treasury), Office of Inspector General (OIG) Semiannual Report summarizing our activities for the 6 month period from April 1, 2006, through September 30, 2006.

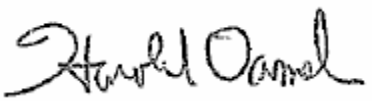
As evidenced by the descriptions on the Highlights In Brief page of the report, we have been very productive and effective over the past 6 months. While the Treasury OIG is, by far, the smallest Cabinet-level Inspector General's office, my staff of approximately 65 auditors and 35 investigators continue to impress me with their productivity, professionalism, and dedication.

As we move forward into Fiscal Year 2007, I plan to continue to utilize my limited audit and investigative resources in the most productive ways possible. I intend to focus our discretionary audit resources in two main areas. Our primary concentration will be on Treasury's management of major capital investments, where there exists a history of problem-plagued and failed projects. We have repeatedly identified this as one of the most serious management challenges facing the Department. Additionally, Congress has also expressed serious concerns about Treasury's track record in executing major Information Technology projects. It is my intention to increase our audit coverage of Treasury's capital investment projects, and perform audit work earlier in the acquisition process, to ensure well-defined project requirements, reasonable cost estimates, satisfactory project management, and a better chance for success.

I also intend to focus audit resources in the area of anti-money laundering and terrorist financing/Bank Secrecy Act (BSA) enforcement. Treasury faces many unique and difficult challenges in carrying out its responsibilities under the BSA, USA Patriot Act, and U.S. foreign sanction programs to prevent and detect money laundering and terrorist financing. Given the criticality of this responsibility, I will continue to devote a significant portion of our audit resources on oversight of the various programs in the Office of Foreign Assets Control, Financial Crimes Enforcement Network, Office of the Comptroller of Currency, and Office of Thrift Supervision.

Turning to our Office of Investigations, we are in the early stages of a proactive improper payment initiative (IPI) which is aimed at identifying and prosecuting those individuals who have fraudulently received Federal benefit payments. My office has oversight of the Financial Management Service which disburses most benefit payments for the federal government. We are currently working jointly with five other Offices of Inspector General combining our resources and sharing information to better detect, and hopefully prevent, this type of fraudulent activity. The initial results from this joint effort have been encouraging. I hope to be able to report some significant progress regarding the IPI in my next Semi-Annual Report.

I very much appreciate the support my staff and I received from former Secretary Snow and his senior staff. In particular, I believe the lines of communication we have developed with Deputy Secretary Kimmitt, Assistant Secretary for Management and Chief Financial Officer Pack, the General Counsel's Office, and a number of the Treasury Bureaus have allowed the OIG to more effectively carry out its mission. I look forward to developing a similar working relationship with Secretary Paulson and the new members of his senior staff, as we seek to continue to identify and prevent potential vulnerabilities and fraud in the Department's programs, promote effective program management, ensure sound financial management, and improve information technology and related security.



Harold Damelin
Inspector General

TABLE OF CONTENTS

This Page Intentionally Left Blank

OVERVIEW OF OIG AND THE TREASURY

The Department of the Treasury's (Treasury) Office of Inspector General (OIG) was established pursuant to the 1988 amendment to the Inspector General Act of 1978, 5 United States Code (U.S.C.) Appendix 3. OIG is headed by an Inspector General (IG) who is appointed by the President of the United States, with the advice and consent of the United States Senate. Serving with the IG in the immediate office is a Deputy Inspector General. OIG performs independent and objective reviews of Treasury programs and operations, except for those of the Internal Revenue Service (IRS), and keeps the Secretary of the Treasury and Congress fully informed of problems, deficiencies, and the need for corrective action. The Treasury Inspector General for Tax Administration (TIGTA) performs audit and investigative oversight related to IRS.

OIG is organized into four divisions: (1) Office of Audit, (2) Office of Investigations, (3) Office of Counsel, and (4) Office of Management.

The **Office of Audit** performs and supervises audits, attestation engagements, and evaluations. The Assistant Inspector General for Audit has two deputies. One deputy is primarily responsible for performance audits, and the other deputy is primarily responsible for financial management and information technology audits. The Office of Audit staff are located in Washington, DC, and Boston, Massachusetts.

The **Office of Investigations** performs investigations and conducts proactive initiatives that are aimed at detecting and preventing fraud, waste, and abuse in Treasury programs and operations. The Office of Investigations also manages the Treasury OIG Hotline System to facilitate the reporting of allegations involving the programs and activities under the auspices of the Department. The Assistant Inspector General for Investigations is responsible for the supervision and conduct of all investigations relating to the Department's programs and operations and performs integrity oversight reviews within select Treasury bureaus. The Office of Investigations is located in Washington, DC.

The **Office of Counsel to the Inspector General** (1) processes all Freedom of Information Act/Privacy Act requests and administrative appeals; (2) processes all discovery requests; (3) represents OIG in administrative Equal Employment Opportunity and Merit Systems Protection Board proceedings; (4) conducts ethics training, provides ethics advice, and ensures compliance with financial disclosure requirements; (5) reviews proposed legislation and regulations; (6) reviews and issues IG subpoenas; (7) reviews and responds to all Giglio requests for information about Treasury personnel who may testify in trials; and (8) provides advice on procurement, personnel, and other management matters and on pending audits and investigations.

The **Office of Management** provides a range of services designed to maintain the OIG administrative infrastructure. These services include: asset management; budget formulation and execution; financial management; information technology; and office-wide policy preparation, planning, emergency preparedness, and reporting for OIG. The Assistant Inspector General for Management is in charge of these functions.

As of September 30, 2006, OIG had 115 full-time staff onboard. OIG's fiscal year 2006 appropriation was $16.8 million.

OIG Values

The values of OIG include producing high-quality products that are accurate, timely, relevant, and responsive to the needs of decision makers. OIG strives to ensure integrity, independence, objectivity, proficiency, and due care in performing its work. OIG promotes teamwork and open communication among its organizational components and encourages and rewards its workforce for innovation, creativity, dedication, and productivity. Finally, OIG fosters an environment of respect, equal opportunity, and diversity among its workforce.

About Treasury

The mission of Treasury is to promote the conditions for prosperity and stability in the United States and encourage prosperity and stability in the rest of the world. Organized into bureaus and offices, Treasury encompasses a wide range of programmatic and operational activities. Currently, Treasury has approximately 112,500 full-time equivalent (FTE) staff. Of this workforce, IRS has approximately 96,700 FTE staff and the other Treasury bureaus and offices have approximately 15,800 FTE staff.

Treasury Bureaus

Alcohol and Tobacco Tax and Trade Bureau (TTB) is responsible for enforcing and administering laws covering the production, use, and distribution of alcohol and tobacco products. It collects alcohol, tobacco, firearms, and ammunition excise taxes totaling approximately $17 billion annually.

Bureau of Engraving and Printing (BEP) designs and manufactures U.S. currency, securities, and other official certificates and awards.

Bureau of the Public Debt (BPD) 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.

Financial Crimes Enforcement Network (FinCEN) 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 (FMS) receives and disburses all public monies, maintains government accounts, and prepares daily and monthly reports on the status of U.S. government finances.

Internal Revenue Service (IRS) is the nation's tax collection agency and administers the Internal Revenue Code.

U.S. Mint (Mint) designs and manufactures domestic bullion, and foreign coins, as well as commemorative medals and other numismatic items. The Mint also distributes U.S. coins to the Federal Reserve Banks and maintains physical custody and protection of the nation's gold and silver assets.

Office of the Comptroller of the Currency (OCC) 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.

Office of Thrift Supervision (OTS) regulates all federal and many state-chartered thrift institutions, which include savings banks and savings and loan associations.

Treasury Offices

Departmental Offices (DO) formulates policy and manages Treasury operations.

Office of Terrorism and Financial Intelligence (TFI) marshals Treasury's intelligence and enforcement functions to safeguard the financial system against illicit use and to combat rogue nations, terrorist facilitators, money launderers, drug kingpins, and other national security threats.

- TFI is headed by an Under Secretary and includes two major components: the **Office of Terrorist Financing and Financial Crime (TFFC)**, responsible for TFI's enforcement functions, and the **Office of Intelligence and Analysis (OIA)**, responsible for TFI's intelligence functions. An Assistant Secretary oversees each of these offices. TFFC is responsible for integrating **FinCEN**, the **Office of Foreign Assets Control (OFAC)**, and the **Treasury Executive Office of Asset Forfeiture (TEOAF)**. TFFC also works in close partnership with **IRS Criminal Investigation (IRS-CI)** to enforce laws against terrorist financing and money laundering, including the Bank Secrecy Act (BSA). OIA supports the formulation of policy and execution of Treasury authorities by providing (1) analysis and intelligence production on financial and other support networks for terrorist groups, proliferators, and other key national security threats, and (2) intelligence support on the full range of economic, political, and security issues. OIA is a member of the United States Intelligence Community.

- **OFAC** administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction. OFAC acts under presidential wartime and national emergency powers, as well as authority granted by specific legislation, to impose controls on transactions and freeze foreign assets under U.S. jurisdiction.

- **TEOAF** administers the **Treasury Forfeiture Fund (TFF)**. TFF is the receipt account for the deposit of nontax forfeitures made by IRS-CI and the Department of Homeland Security, including U.S. Immigration and Customs Enforcement, U.S. Customs and Border Protection, U.S. Secret Service, and U.S. Coast Guard. Funding for participating law enforcement agencies is provided through TFF to enhance their capabilities to conduct successful investigations and forfeitures. TFF's mission is to affirmatively influence the consistent and strategic use of asset forfeiture by participating agencies to disrupt and dismantle criminal enterprises.

Office of International Affairs advises on and assists in the formulation and execution of U.S. international economic and financial policy. Responsibilities of the Office of International Affairs include developing policies and guidance in the areas of international financial, economic, monetary, trade, investment, bilateral aid, environment, debt, development, and energy programs, including U.S. participation in international financial institutions.

Exchange Stabilization Fund (ESF) is used to purchase or sell foreign currencies, hold U.S. foreign exchange and Special Drawing Rights assets, and provide financing to foreign governments. All ESF operations require the explicit authorization of the Secretary of the Treasury.

Community Development Financial Institutions Fund (CDFI Fund) expands the availability of credit, investment capital, and financial services in distressed urban and rural communities.

Federal Financing Bank (FFB) provides federal and federally assisted borrowing, primarily to finance direct agency activities such as construction of federal buildings by the General Services Administration (GSA) and meeting the financing requirements of the U.S. Postal Service.

Office of DC Pensions makes federal benefit payments associated with the District of Columbia (DC) Retirement Programs for police officers, firefighters, teachers, and judges.

Air Transportation Stabilization Board was authorized to issue federal credit instruments (loan guarantees) to assist air carriers that suffered losses as a result of the terrorist attacks on the United States that occurred on September 11, 2001. This authority expired September 30, 2004. As of September 30, 2006, approximately $18 million in loan guarantees were outstanding.

TREASURY MANAGEMENT AND PERFORMANCE CHALLENGES

In accordance with the Reports Consolidation Act of 2000, the IG annually provides the Secretary of the Treasury with OIG's perspective on the most serious management and performance challenges facing the Department. Among other things, the Secretary must include these challenges in the Department's annual Performance and Accountability Report. In October 2005, the IG reported five challenges to former Secretary Snow that we believe seriously impeded the Department's ability to conduct its program responsibilities and ensure the integrity of its operations. These challenges are: (1) Corporate Management, (2) Management of Capital Investments, (3) Information Security, (4) Linking Resources to Results, and (5) Anti-Money Laundering and Terrorist Financing/Bank Secrecy Act Enforcement. In a memorandum dated October 16, 2006, the IG reported to Secretary Paulson that while some progress on each of these five challenges has been made, they continue to represent significant risks to the Department.

The five management and performance challenges are summarized below:

- Corporate Management This is an overarching management challenge. Treasury needs to provide effective corporate leadership in order to resolve serious bureau and program office deficiencies that adversely impact the performance of Treasury as a whole. In particular, Treasury needs to assert strong leadership and supervision over the IRS to resolve the longstanding material weaknesses and system deficiencies that hamper the timely and reliable information necessary to effectively manage IRS operations. In addition, while progress has been made, the Department has not fully implemented a corporate-level control structure to ensure that capital investments are properly managed, information about government operations and citizens is adequately secured, and financial resources used by Treasury can be linked to its operational results. The increasing emphasis on agency-wide accountability envisioned in the management reform legislation of the past decade and the President's Management Agenda, has underscored the need for effective corporate management at Treasury. With nine bureaus and many program offices, Treasury is a highly decentralized organization. As such, Treasury management should ensure consistency, cohesiveness, and economy among all bureaus and program offices in achieving Treasury's goals and objectives.

  This past year, we noted that the Department's senior leadership has asserted more direct and substantive involvement in developing and implementing Treasury-wide polices and initiatives across a number of fronts. Also, the Deputy Secretary recently issued a memorandum requiring that internal control programs (programs to ensure accountability and promote effective management and stewardship) be included in all fiscal year 2007 senior leadership performance plans. In the future, this type of direct involvement by senior leadership needs to be maintained so that progress continues.

- Management of Capital Investments Treasury needs to better manage large acquisitions of mission-critical systems and other capital investments. In the past, serious problems have been identified with the Treasury Communications Enterprise (TCE) procurement, Treasury's HR Connect system, and the Treasury and Annex Repair and Restoration project. This year, we note continuing issues with TCE and new problems have been brought to light with BSA Direct, and the web-based Electronic Fraud Detection System

(Web EFDS). Specifically, as discussed in our prior semiannual report, we found that the TCE procurement, estimated to cost $1 billion over its useful life, was poorly planned, executed, and documented. Treasury amended and reopened the TCE solicitation in October 2005, but has yet to award the TCE contract. In July 2006, after nearly 2 years in development and $15 million spent, FinCEN terminated its contract for the storage and retrieval component of BSA Direct after significant concerns were raised about schedule delays and project management. IRS had similar problems with Web EFDS, a system costing more than $20 million intended to prevent fraudulent refunds. In April 2006, after a significant delay, IRS stopped all development activities for Web EFDS. IRS also was unable to use EFDS to prevent fraudulent refunds during processing year 2006. The TIGTA reported that without Web EFDS, more than $300 million in fraudulent refunds may have been allowed.

The Deputy Secretary recently emphasized the need to better manage information technology capital investments to the heads of Treasury bureaus, noting that this is a responsibility of all senior management and not just that of the Chief Information Officer. Involvement and accountability at the top is a critical factor to ensure the successful implementation of systems.

- Information Security Despite some notable accomplishments, the Department needs to improve its information security program and practices to achieve compliance with the Federal Information Security Management Act of 2002 (FISMA) and Office of Management and Budget (OMB) requirements. In the past, we reported that Treasury's systems inventory was not accurate, complete, or consistently reported. During the past year, the Department overcame this weakness in its security program by providing direction to the bureaus in developing a Department-wide inventory of information systems. Although the Department still needs to implement additional actions to further improve the system inventory, we believe the inventory is substantially complete and generally conforms to applicable requirements. Nevertheless, we reported that information security deficiencies at Treasury, in the aggregate, constitute substantial noncompliance with FISMA. Improvements are needed in a number of areas such as certification and accreditation, tracking corrective actions, and incident response. Also, during 2006 OMB required agencies to perform specific actions to protect certain personally identifiable information. Treasury faces significant challenges to meet these requirements. In this regard, the Department needs to ensure that security controls pertaining to personally identifiable information are addressed Treasury-wide. In a July 2006 memorandum to Treasury bureaus, the Department provided implementation guidance and required bureaus to identify their specific actions taken and planned, including dates, to address weaknesses in security controls pertaining to personally identifiable information.

- Linking Resources to Results Because the Department has not fully developed and incorporated managerial cost accounting (MCA) into its business activities, the Department cannot adequately link financial resources to operating results. This inhibits comprehensive program performance reporting and meaningful cost benefit analyses of the Department's programs and operations. MCA involves the accumulation and analysis of financial and non-financial data, resulting in the allocation of costs to organizational pursuits such as

performance goals, programs, activities, and outputs, and should be a fundamental part of a financial/performance management system. In response to a critical Government Accountability Office report on MCA at Treasury, the Department developed a high-level MCA implementation plan. This plan focuses on (1) clarifying and reaffirming the Department's MCA policy for all bureaus; (2) identifying MCA needs across the Department; (3) ensuring MCA needs are linked to the Department's strategic plan, budget, and performance measures; (4) identifying gaps between Department and bureau needs and existing MCA capabilities; and (5) developing plans to eliminate these gaps. However, none of the specific action items in the plan have been completed and target dates for certain actions have been missed.

- Anti-Money Laundering and Terrorist Financing/Bank Secrecy Act Enforcement Treasury faces unique challenges in carrying out its responsibilities under the Bank Secrecy Act (BSA) and USA Patriot Act to prevent and detect money laundering and terrorist financing. To effectively prevent and detect financial crimes and terrorist financing it is necessary to have: (1) strong control environments at financial institutions that ensure that business is conducted with reputable parties, and large currency transactions and suspicious activities are properly and timely reported to Treasury; (2) strong federal and state regulatory agencies that examine and enforce BSA and USA Patriot Act requirements at financial institutions; and (3) strong analytical capacity to identify and refer to law enforcement, leads provided through reports filed by financial institutions. While FinCEN is the Treasury bureau responsible for administering BSA, it relies on other Treasury and non-Treasury agencies to enforce compliance with the Act's requirements. OFAC, the Treasury office responsible for administering U.S. foreign sanction programs, also relies on other Treasury and non-Treasury agencies to ensure compliance with OFAC requirements. Past audits and Congressional hearings, however, have surfaced serious regulatory gaps in the detection of and/or timely enforcement action against financial institutions for BSA and related violations. In an attempt to improve compliance and address some of these gaps, Treasury created TFI through which FinCEN and OFAC now report. In addition, FinCEN, beginning in 2004, (1) created a compliance office to improve BSA oversight and coordination with financial institution regulators, and (2) entered into memoranda of understanding (MOUs) with the federal banking regulators, IRS, and most states to enhance communication and coordination.

  During this semiannual period, we completed audits at FinCEN, OCC, and OTS related to this management challenge, which are discussed in the next section of this report. Given the criticality of this management challenge to the Department's mission, we will continue to devote a significant portion of our audit resources to this management challenge.

FINANCIAL MANAGEMENT

Financial Audits

The Chief Financial Officers (CFO) Act, as amended by the Government Management Reform Act of 1994 (GMRA), requires annual financial statement audits of Treasury and Office of Management and Budget (OMB)-designated entities. In this regard, OMB has designated IRS for annual financial statement audits. The financial statements of certain other Treasury component entities are audited pursuant to other requirements, or because of their materiality to Treasury's consolidated financial statements. The following table shows audit results for fiscal years 2005 and 2004.

Treasury Audited Financial Statements and Related Audits

	Fiscal Year 2005 Audit Results			Fiscal Year 2004 Audit Results		
Entity	**Opinion**	**Material Weakness**	**Other Reportable Conditions**	**Opinion**	**Material Weakness**	**Other Reportable Conditions**
GMRA/CFO Act Requirements						
Treasury Department	UQ	1	1	UQ	1	1
IRS (A)	UQ	4	2	UQ	4	2
Other Required Audits						
BEP	UQ	0	1	UQ	0	0
CDFI Fund	UQ	0	0	UQ	0	0
Office of DC Pensions	UQ	0	0	UQ	0	0
ESF	UQ	0	0	UQ	0	0
FFB	UQ	0	0	UQ	1	0
OCC	UQ	0	0	UQ	0	1
OTS	UQ	0	0	UQ	0	0
TFF	UQ	1	1	UQ	0	1
Mint						
Financial Statements	(B)	(B)	(B)	UQ	0	0
Custodial Gold and Silver Reserves	UQ	0	0	UQ	0	0
Material to Treasury Department Financial Statements						
BPD						
Schedule of Federal Debt (A)	UQ	0	0	UQ	0	0
Government Trust Funds	UQ	0	0	UQ	0	1
FMS						
Treasury Managed Accounts	UQ	0	0	UQ	0	0
Operating Cash of the Federal Government	UQ	0	1	UQ	0	1
Other						
FinCEN	UQ	1	0	N/A	N/A	N/A

UQ Unqualified opinion
N/A Bureau was not audited before fiscal year 2005
(A) Audited by the U.S. Government Accountability Office.
(B) On June 28, 2006, we issued the independent public accountant's (IPA) audit report on the Mint's fiscal year 2005 financial statements. In July 2006, we recalled the report at the request of the Mint Acting Director because he wanted to change his letter that accompanied the financial statements. That request and certain other circumstances necessitated the IPA to perform additional audit work. As of September 30, 2006, the audit was still in progress.

Audits of the fiscal year 2006 financial statements or schedules of the Department and component reporting entities were in progress at the end of this semiannual reporting period.

Federal Financial Management Improvement Act (FFMIA) of 1996

The following instances of FFMIA noncompliance were reported in connection with the audit of the Department's fiscal year 2005 consolidated financial statements. All instances relate to IRS. The current status of these FFMIA noncompliances, including progress in implementing remediation plans, will be evaluated as part of the audit of Treasury's fiscal year 2006 financial statements.

Entity	Condition	Fiscal Year First Reported for FFMIA Purposes	Type of Noncompliance
IRS	Financial management systems do not provide timely and reliable information for financial reporting and preparation of financial statements. IRS had to rely extensively on resource-intensive compensating procedures to generate reliable financial statements. IRS also lacks a subsidiary ledger for its unpaid assessments and lacks an effective audit trail from its general ledger back to subsidiary detailed records and transaction source documents for material balances such as tax revenues and tax refunds.	1997	Federal Financial Management Systems Requirements
IRS	Deficiencies were identified in information security controls, resulting in increased risk of unauthorized individuals being allowed to access, alter, or abuse proprietary IRS programs and electronic data and taxpayer information.	1997	Federal Financial Management Systems Requirements
IRS	Material weaknesses were identified related to controls over unpaid tax assessments and tax revenue and refunds.	1997	Federal Accounting Standards
IRS	Financial management system cannot routinely accumulate and report the full costs of its activities.	1998	Federal Accounting Standards
IRS	General ledger system is not supported by adequate audit trails and is not integrated with its supporting records for material balances such as tax revenues and tax refunds.	1997	Standard General Ledger

Attestation Engagements

The following engagements were completed in support of the audit of Treasury's fiscal year 2006 consolidated financial statements. These engagements also support the financial statement audits of certain other federal agencies.

BPD Controls over the Processing of Transactions for Other Agencies

An IPA, under our supervision, examined the general computer and accounting controls related to certain services provided by BPD's Administrative Resource Center to various federal agencies (customer agencies). The IPA found that (1) BPD's description of controls for these activities fairly presented, in all material respects, the controls that had been placed in operation as of June 30, 2006, (2) the controls were suitably designed, and (3) the controls tested by the IPA were effective during the period July 1, 2005, to

June 30, 2006. The IPA noted no instances of reportable noncompliance with laws and regulations tested. **(OIG-06-035)**

An IPA, under our supervision, performed examinations that covered the general computer and trust fund management processing controls related to BPD's transactions processing of investment accounts of various federal and state government agencies (program entities) and the general computer and investment/redemption processing controls related to the BPD's transactions processing of investment accounts for various federal government agencies (fund agencies). The IPA found that (1) BPD's description of these controls fairly presented, in all material respects, the controls that had been placed in operation as of July 31, 2006, (2) the controls were suitably designed, and (3) the controls tested by the IPA were effective during the period August 1, 2005, to July 31, 2006. The IPA noted no instances of reportable non-compliance with the laws and regulations tested. **(OIG-06-038 and OIG-06-039)**

INFORMATION TECHNOLOGY

Evaluation of Treasury's Federal Information Security Management Act Implementation for 2006

Despite notable progress, Treasury has deficiencies that, in the aggregate, constitute substantial noncompliance with FISMA.

The Federal Information Security Management Act of 2002 (FISMA) requires an annual independent evaluation of Treasury's information security program and practices. To meet FISMA requirements, we contracted with KPMG LLP, an independent certified public accounting firm, to perform the FISMA evaluation of Treasury's unclassified systems, except for those of the IRS. TIGTA performed the FISMA evaluation for the IRS systems. OIG auditors performed the FISMA evaluation of Treasury's national security systems.

Despite notable progress, Treasury has deficiencies that, in the aggregate, constitute substantial noncompliance with FISMA. The most important of these deficiencies are:

- Non-IRS bureaus and offices within Treasury have significant deficiencies in their information security program and practices. KPMG LLP reported concerns in the following areas at various bureaus: certification and accreditation, training, plans of actions and milestones, system interfaces, security self-assessments, system categorization, configuration management process, and incident response process.
- IRS also continues to have shortcomings in its information security program and practices. TIGTA reported significant deficiencies in the following areas: continuous monitoring of systems, incident reporting procedures, and training employees with key security responsibilities.
- We reported several matters pertaining to national security systems.

We also identified areas where Treasury improved its information security program and practices. Most notably, Treasury now has complete and properly categorized inventories of its national security systems. We also generally agree with the Office of the Chief Information Officer on the total number of Treasury systems. In addition, we noted in our FISMA evaluation report that TIGTA reported that IRS has made steady progress in complying with FISMA requirements. **(OIG-CA-06-004, OIG-CA-06-005, and OIG-CA-06-008)**

Effective Security Controls Needed to Mitigate Critical Vulnerabilities in OCC's Networked Information Systems

We determined that several high-risk vulnerabilities may expose OCC's network and systems to unauthorized access and exploitation.

In support of FISMA, we completed an audit of network and system security at OCC to check for vulnerabilities in OCC's network communication services, operating systems, routers, servers, and applications. OCC's network and systems are integral parts of its mission support structure. An unauthorized attack or system intrusion on OCC's network and computer systems could be detrimental to its mission.

We determined that several high-risk security vulnerabilities may expose OCC's network and systems to unauthorized access and exploitation. In addition, we provided recommendations to address those vulnerabilities. Because of the sensitivity of these vulnerabilities and recommendations, we designated the report "limited official use."

OCC management concurred with our recommendations. Where possible, device or software specific vulnerabilities cited in the report were corrected. In other cases, OCC management provided plans for corrective actions to mitigate the vulnerabilities. **(OIG-06-040)**

OCC's Disaster Recovery Exercises Were Successful but Certain Procedures Need to be Improved

Although OCC successfully met the primary objectives for the two DREs, we found that improved procedures are needed to restore applications.

In 2005, OCC hired a contractor to provide disaster recovery services for its information systems. OCC is in the initial phase of developing its disaster recovery capability with its contractor, which provides recovery facilities, hardware, software, services, and technical personnel for OCC recovery exercises. During 2006, we observed two disaster recovery exercises (DREs) at two different locations.

Although OCC successfully met the primary objectives for the two DREs, we found that improved procedures are needed to restore applications. OCC concurred with our recommendation to ensure that the procedures for restoring applications are sufficient, and has taken or planned corrective action. Because of the sensitivity of the finding and

recommendation, we designated our reports on the DREs "limited official use." **(OIG-06-041 and OIG-06-042)**

Security Testing of Networked Systems

During the period, OIG acquired software tools and its information technology audit staff obtained training to perform security tests of networked systems. To pilot the use of these tools, we performed tests of OIG's network noting certain weaknesses. Those weaknesses are being corrected or mitigated. We plan to perform similar tests of networked systems at selected Treasury bureaus in the future.

PROGRAMS AND OPERATIONS

OCC Did Not Take Formal Enforcement Action Against Wells Fargo Bank for Significant Bank Secrecy Act Deficiencies

In 2005, OCC took enforcement action against Wells but instead of issuing a cease and desist order, it issued an informal, nonpublic action.… We believe OCC's failure to take formal enforcement action against Wells sent the wrong message to the banking industry about OCC's resolve to ensure that banks comply with BSA.

OCC's examiners found numerous and recurring deficiencies in Wells Fargo Bank's (Wells) BSA compliance program from 1999 through 2004. Among the deficiencies identified were (1) weak internal controls over the program, (2) inadequate independent testing of business lines, (3) lack of BSA oversight, and (4) failure to file suspicious activity reports (SAR) in accordance with regulations and program requirements. Federal law (12 U.S.C. 1818) *requires* financial institution regulators, such as OCC, that identify violations in BSA programs to take formal enforcement action by issuing the institution a public cease and desist order. In 2005, OCC took enforcement action against Wells but instead of issuing a cease and desist order, OCC issued an informal, nonpublic action that addressed BSA deficiencies as safety and soundness weaknesses at the bank. This action required the bank to submit, and get approved, a plan for improvement.

OCC senior management did not disagree with the examiners' findings that the bank had BSA program deficiencies, but believed that the deficiencies did not rise to the level of a program violation. They also believed that examiners' communications with the bank may have left an unclear message about the seriousness of the problems found. However, we found that examination reports provided to Wells clearly documented significant weaknesses and deficiencies in Wells's BSA program and concluded that OCC should have acted more quickly and forcefully to require Wells to strengthen its BSA compliance. We believe that OCC's failure to take formal enforcement action against Wells sent the wrong message to the banking industry about OCC's resolve to ensure that banks comply with BSA.

We also found that OCC did not follow its usual practice when determining what enforcement action to take. OCC guidelines require that the planned enforcement action be presented to the Washington Supervision Review Committee (WSRC), a headquarters committee consisting of selected senior officials with a cross-section of OCC knowledge and expertise. However, WSRC input was not sought and WSRC was effectively removed from the customary enforcement process.

In addition, OCC did not keep FinCEN fully informed of the ongoing enforcement action, in accordance with a September 2004 MOU between OCC and FinCEN. Under the MOU, OCC is to promptly notify FinCEN when significant BSA violations are found at an institution. While OCC advised FinCEN early on that it was considering a cease and desist order against Wells, it did not inform FinCEN that it changed course to issue the informal action until after that action was taken. As a result, FinCEN was not afforded the opportunity to timely review the findings or participate in the enforcement process.

While OCC advised FinCEN early on that it was considering a cease and desist order against Wells, it did not inform FinCEN that it changed course to issue the informal action until after that action was taken.

We also reported that since the Wells enforcement action, OCC has renewed its emphasis on Bank Secrecy Act/Anti-Money Laundering (BSA/AML) compliance by national banks. In November 2005, the Comptroller of the Currency announced his plans to enhance OCC's supervision of the bank compliance programs. These initiatives are designed to strengthen OCC's BSA program examinations, enhance resources and expertise devoted to BSA supervision, and provide clear expectations about OCC's BSA/AML supervision to the industry.

With regard to Wells, we recommended that OCC closely monitor Wells's compliance with the improvement plan, take prompt enforcement action should the bank fail to comply, and keep FinCEN fully informed of the bank's progress in improving compliance. We also recommended specific actions OCC should take to improve its handling of bank noncompliance with BSA in the future. These actions include obtaining WSRC input before taking enforcement action and documenting the WSRC deliberation and basis for the enforcement action taken. OCC concurred with our recommendations. **(OIG-06-034)**

FinCEN Took Steps to Better Analyze BSA Data But Challenges Remain

…we reviewed FinCEN's analytic data for fiscal years 2003 through the first quarter of 2005 and found that FinCEN had made limited progress in increasing its complex data mining and analysis (i.e., proactive case work).

The USA Patriot Act requires FinCEN to furnish research, analytical, and informational services to financial institutions and appropriate law enforcement authorities to fight terrorism, organized crime, and money laundering. In this regard, an objective in FinCEN's fiscal years 2006-8 strategic plan was to adjust its support of law enforcement investigations by performing complex data mining and analysis.

FinCEN planned to increase its analytic products while reducing time spent in routine data retrieval. This strategy was designed to shift FinCEN's effort from routine data retrieval (reactive cases) to complex data mining (proactive cases).

We conducted an audit to determine the extent to which FinCEN performed complex analyses of BSA and other data intended to provide law enforcement with new leads or clues regarding individuals, entities, and organizations engaging in terrorist acts or money laundering. We found FinCEN has taken steps to increase its use of analytic tools and methods for identifying trends and patterns in BSA data. However, we reviewed FinCEN's analytic data for fiscal years 2003 through the first quarter of 2005 and found that FinCEN had made limited progress in increasing its complex data mining and analysis (i.e., proactive case work). Proactive case work increased during this period, from 6 percent of FinCEN's analytical case work in 2003 to 10 percent in 2005. Filing law enforcement requests for specific information, known as reactive case work, continued to be FinCEN's focus. We found that FinCEN's effort to conduct more complex analysis was hindered during 2004 and 2005 when it released a number of contract employees who did not meet upgraded FinCEN security clearance requirements. These contract employees had been handling about a third of FinCEN's reactive case work and, upon release, this work was reassigned to FinCEN's analysts.

We also found that FinCEN's database to track and report the number of investigative cases, subjects, and strategic analytic products was not accurate or reliable. The database did not always contain information about the timeliness of work or resources used. Data problems resulted from a combination of system weaknesses that made it difficult to develop summary data, and data recording errors that occurred when analysts did not record data in accordance with standard operating procedures. FinCEN also made changes in how data were categorized from year to year.

Finally, we found that certain internal controls over BSA and law enforcement data were weak and could allow these data to be compromised. First, FinCEN had yet to schedule on-site security inspections at a number of law enforcement agencies with remote access to BSA data through FinCEN's Gateway system. Second, FinCEN had neither a policy nor a methodology to review internal analyst queries for possible misuse or abuse or to prevent and detect browsing of BSA and law enforcement data. Third, after FinCEN increased the security level requirement for its contract employees, they were still allowed to access sensitive BSA and other data, even though they had not yet obtained the proper clearances.

We recommended that FinCEN develop a strategy to implement FinCEN's goal of performing more complex analysis, have a mechanism for periodically assessing its progress in achieving its strategic goals and objectives, and enhance its current database system or acquire a new system. To improve FinCEN's data security controls, we recommended that FinCEN (1) continue to monitor the scheduling and completion of its onsite inspections of Gateway users, (2) establish a policy to address inappropriate browsing of databases with a methodology to monitor system activity, and (3) conduct a risk assessment of the contract employees' use of FinCEN's systems to ensure that they

conducted appropriate research and case support. FinCEN concurred with our recommendations and has either completed action or established target dates for completion. **(OIG-06-030)**

OCC's and OTS's Examinations of Financial Institutions With OFAC Foreign Sanctions Programs

OFAC administers and enforces economic and trade sanctions against targeted foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction. In accordance with these sanctions, financial institutions are required to block or reject any transactions involving individuals, companies, or other organizations with a link to these entities. Lacking direct authority, OFAC relies on financial institution regulators to ensure compliance. The regulators, however, manage their compliance examinations independently from OFAC and are prevented from sharing information with OFAC.

…OCC's and OTS's OFAC examination work papers did not provide assurance that national banks and federal and state-chartered thrift institutions were adequately reviewing or effectively administering OFAC's foreign sanctions programs.

As part of a broader, ongoing OIG audit of OFAC's administration of its sanctions programs, we tested regulator oversight for a sample of financial institutions examined by OCC and OTS. We found that OCC's and OTS's OFAC examination work papers did not provide assurance that national banks and federal and state-chartered thrift institutions were adequately reviewing or effectively administering OFAC's foreign sanctions programs. We found, for every examination sampled, one or more instances in which documentation was insufficient to verify that examiners adequately assessed OFAC program compliance. Specifically, the OCC examination workpapers did not always contain sufficient documentation to demonstrate that examiners fully assessed (1) bank policies and procedures for its OFAC compliance program, (2) bank comparisons of its accounts with OFAC listings, (3) correspondence between the bank and OFAC, and (4) results of internal bank audits for possible OFAC program concerns. Similarly, the OTS examination work papers did not always contain sufficient documentary evidence to demonstrate that examiners fully assessed (1) policies and procedures for the OFAC compliance program, (2) internal audit results for possible OFAC program concerns, and (3) OFAC penalty or warning notices that had been sent to thrifts.

OCC officials agreed with the observations, but noted that OCC's policy on supervisory workpapers states that examiners should generate and retain only those documents necessary to support the scope of supervisory activity, significant conclusions, rating changes, or changes in risk profile. OTS's policy is that documentation of OFAC examinations is generally minimal unless a problem is noted. OTS's examination workpapers are "exception-based." We believe, however, that these policies make it difficult to assess the adequacy of the reviews and create inconsistency in how program results are documented.

We made recommendations to OCC and OTS to ensure that their examiners use OFAC examination guidelines contained in the Federal Financial Institutions Examination Council *Bank Secrecy Act/Anti-Money Laundering Manual*, issued in June 2005. We also recommended that examiners better document their planning, work performed and significant conclusions in their workpapers.

In their replies to the reports, OCC and OTS both recognized the need to better document their OFAC examination work. OCC concluded that the level of exceptions noted in our audit report pointed to a need for improvement in practice. In this regard, OCC will reinforce its expectations with examination staff. OTS agreed to issue and implement examiner guidance to ensure enhancement of OFAC procedures in the fourth calendar quarter of 2006. **(OIG-06-033** and **OIG-06-044)**

The Mint Needs to Determine Whether Its Long-Delayed A-76 Competition for Coin Blank Production Should Be Continued

Nearly 3 years since the competition was first announced and 1 year since the competition was re-announced, the Mint is still not close to completing the BAU competition. The reasons for the Mint's delays in completing the BAU competition are numerous, but mostly due to poor planning by the Mint….

OMB Circular No. A-76 (Revised), *Performance of Commercial Activities* (Circular A-76), reiterates the longstanding policy of the federal government to rely on the private sector for needed commercial services. In general, Circular A-76 requires that federal agencies identify activities performed by government personnel as either commercial or inherently governmental. As appropriate, agencies are then to use a competition to determine whether government personnel should perform a commercial activity. During the period, we issued a second audit report on the Mint's standard A-76 competition for its blanking, annealing, and upsetting (BAU) manufacturing process to produce coin blanks. As in our prior audit report (issued October 2004), we concluded that the Mint did not adequately plan or implement this competition.

The Mint publicly announced the BAU competition in October 2003 but did not complete the competition within the 1-year timeframe required by Circular A-76. The Mint subsequently obtained an OMB-approved deviation to certain Circular A-76 requirements in July 2005 and, in turn, re-announced the competition in September 2005. Nearly 3 years since the competition was first announced and 1 year since the competition was re-announced, the Mint is still not close to completing the BAU competition.

The reasons for the Mint's delays in completing the BAU competition are numerous, but mostly due to poor planning by the Mint, both at the outset of the competition in 2003 and after the OMB-approved deviation last year. Some of the deficiencies we noted in the Mint's planning and implementation of the competition include the following: (1) hiring a contractor to develop the Performance Work Statement (PWS), and then changing it, (2) publishing a PWS with errors in the specifications for coin blanks, (3) not addressing Circular A-76 requirements concerning Government Furnished Property requirements or the

use of potential excess space, (4) not addressing security issues in the draft PWS or draft solicitations, and (5) issuing a draft Mint directive for conducting A-76 competitions but not following its guidelines.

Given the significant actions still needed by the Mint to address these and other deficiencies, we recommended that the Mint expeditiously complete a formal business case analysis to determine whether the activity should continue to be competed. Mint management concurred with this recommendation and provided a target date of December 31, 2006, for completing the business case analysis and deciding on an appropriate course of action properly supported by the analysis.

It should be noted that we undertook our audit of the BAU competition to address a requirement in House Conference Report (H. Rep. 108-401) for the Consolidated Appropriations Act, Fiscal Year 2004, which directed our office to perform a study on the potential and cost-effectiveness of expanded use of coin blanks in the production of circulating coins. However, we informed the Committees on Appropriations in March 2004 that since the Mint had already publicly announced the BAU competition, the study as described in the Report could not be performed. Instead, we advised the Committees that we would audit the Mint's compliance with Circular A-76 in carrying out the competition. **(OIG-06-036)**

TTB's Risk Model for Selecting Taxpayers for Audit Could Be Improved

We reviewed the fiscal year 2005 risk model and found that it contained errors which resulted in the assignment of incorrect risk rating scores to some large taxpayers.

The TTB strategic plan for fiscal years 2003 through 2008 calls for its Tax Audit Division (TAD) to move from random selection of audit targets to risk-based selection. To achieve this goal, TAD developed a risk model that includes a variety of factors, with a major emphasis on revenue. TAD focused its audits on the largest taxpayers in a cycle that would complete audits of all large taxpayers in 5 years. These taxpayers accounted for approximately 98 percent of all excise taxes collected. Using this strategy, TAD reported about $17.1 million in additional taxes due or collections from 110 completed audits in fiscal year 2005.

We reviewed the fiscal year 2005 risk model and found that it contained errors that resulted in the assignment of incorrect risk rating scores to some large taxpayers. We also could not easily reconcile certain source data with the data found in the risk model. While attempting to verify risk model data at TTB's National Revenue Center, we found that individual taxpayer account balances may be inaccurate because of a federal excise tax system control weakness in the processing of electronic fund transfer payments to individual taxpayer accounts. TTB is currently working to resolve this problem.

TTB concurred with our recommendations addressing the use of the risk model to select taxpayers for audit, the accuracy of data in the risk model, and controls over electronic funds transfer payments. **(OIG-06-043)**

Individual Pleads Guilty to Defrauding Federal Emergency Management Agency

*Jeffrey Rothschild pled guilty in the U.S. District Court for the District of Columbia, to a three-count criminal information charging him with bank fraud, mail fraud, and money laundering from September to December 2005, in connection with a scheme to defraud FEMA of more than $100,000 in relief funds intended for victims of Hurricanes Katrina and R*ita.

On August 28, 2006, Jeffrey Rothschild pled guilty in the U.S. District Court for the District of Columbia, to a three-count criminal information charging him with bank fraud, mail fraud, and money laundering from September to December 2005. He was involved in a scheme to defraud the Federal Emergency Management Agency (FEMA) of more than $100,000 in relief funds intended for victims of Hurricanes Katrina and Rita. The payments were made through FMS.

Rothschild's arrest on June 27, 2006, in El Paso, Texas, was the result of a joint investigative effort by Treasury OIG, the DC Metro Area Fraud Task Force, the United States Postal Inspection Service, the U.S. Secret Service, and the Department of Homeland Security OIG. Rothschild confessed to committing approximately $100,000 in FEMA Katrina/Rita benefits fraud, $40,000 to $50,000 in credit card fraud, and $40,000 in a check kiting scheme, through the use of fraudulent identities. Sentencing for Rothschild is scheduled for December 1, 2006. He faces between 84 and 105 months in prison under federal sentencing guidelines.

This case was highlighted in the first annual report of the Hurricane Katrina Fraud Task Force prepared by the Department of Justice.

DC Resident Pleads Guilty to Hurricane Katrina Fraud

DC resident, Charles Washington ...falsely claimed that he rented and was living in a single-family residence in New Orleans, LA, during Hurricane Katrina….

As part of the Attorney General's and President's Council on Integrity and Efficiency's commitment to combat fraudulent schemes related to Hurricanes Katrina and Rita, OIG led the investigation of a case against a DC resident, Charles Washington, for making a false statement on a FEMA application. Washington falsely claimed that he rented and was living in a single-family residence in New Orleans, LA, during Hurricane Katrina, that his home was damaged, and that he lost personal property as a result of the hurricane. He received three Treasury checks totaling $14,749. Washington pled guilty on June 13, 2006, in the U.S. District Court for the District of Columbia, to a false statement charge. Washington is scheduled for sentencing on November 7, 2006, and faces a maximum of 5 years imprisonment.

BEP Employee Stole Partially Printed $100 Federal Reserve Notes

Treasury OIG special agents, with the assistance of BEP investigators and personnel from the U.S. Secret Service, recovered more than 180 of these notes from the Philadelphia Federal Reserve Bank and various casinos in Delaware, New Jersey, and West Virginia.

In May 2006, BEP notified OIG that at least 64 incomplete $100 notes, missing the Treasury seal and serial number, had entered into commerce. As the integrity of U.S. currency is a significant Departmental responsibility, Treasury OIG special agents, with the assistance of BEP investigators and the U.S. Secret Service, commenced an investigation which led to the recovery of more than 180 of these notes from the Philadelphia Federal Reserve Bank and various casinos in Delaware, New Jersey, and West Virginia. It was quickly determined that 672 partially printed $100 notes (originating from 21 32-count sheets) were stolen from the BEP's Eastern Currency Facility in Washington, DC. The Federal Bureau of Investigation (FBI) subsequently joined the investigation.

Surveillance video from a Delaware casino disclosed the passing of several of the partially printed notes and led to the identification of a BEP employee, David Faison, a stock control recorder. Additional surveillance of Faison's activities resulted in search warrants being obtained for his residence, vehicle, and BEP locker. The execution of the search warrant at Faison's residence resulted in the recovery of nine of the 32-count sheets and one partial sheet consisting of 24 partially printed $100 notes. Faison was subsequently arrested by Treasury OIG and FBI special agents. On September 6, 2006, pursuant to a plea agreement, Faison pled guilty to one count of possession of tools and materials for counterfeiting purposes. He is presently awaiting sentencing and the investigation remains ongoing in order to validate admissions made by Faison.

OIG Proactive Investigative Initiative Identified Improper Worker's Compensation Payments

As part of an Inspector General-wide proactive project to identify potential fraudulent Federal Employee Workers' Compensation (FECA) claims, an OIG investigation revealed that the daughter of a deceased BEP employee improperly received $18,206 in FECA payments after the employee's death. The daughter took the money from the deceased employee's bank account and deposited some of the funds into a Certificate of Deposit under her name. As a result of our investigation, the individual arranged to repay the money, and the deceased employee's name was removed from the Department of Labor's Office of Workers Compensation payment rolls preventing potential future improper payments of $21,570.

Inquiry Into an Alleged Conflict of Financial Interest by Former Secretary Snow

In response to a referral from a member of Congress, OIG conducted an inquiry into a possible violation of Title 18 U.S.C. § 208 (conflict of financial interest) by then Secretary

of the Treasury, John Snow. The issue arose because of the former Secretary's membership on the Committee on Foreign Investment in the United States and its January 2006 approval of Dubai Ports World's (DPW) planned acquisition of Peninsular and Oriental Steam Navigation Company (P&O). Because DPW had acquired CSX World terminals in February 2005 from the CSX Corporation (the Secretary's former employer), it was alleged in the referral that Secretary Snow might benefit from DPW's acquisition of P&O.

The inquiry disclosed that Secretary Snow maintained limited financial ties to CSX in the form of a life insurance policy, a fixed pension, and a deferred compensation plan, and these items were included in his public financial disclosure reports. The former Secretary had divested himself of his other financial interests in CSX by April 2003, and stood to bear no financial gain from CSX's sale of CSX World Terminals to DPW. The inquiry concluded no conflict of interest by Secretary Snow. It should be noted that DPW later decided not to complete the acquisition of P&O.

Former Navy Program Manager Imprisoned for Contract Fraud

John Dyer, a former Navy Program Manager, covertly arranged for his wife to be employed under a contract awarded by a component of the Treasury Franchise Fund.

A joint investigation by OIG and the Naval Criminal Investigative Service disclosed that John Dyer, a former Navy program manager, covertly arranged for his wife to be employed under a contract awarded by a component of the Treasury Franchise Fund. In doing so, Dyer manipulated the contracting process and caused the government to pay the contractor $81,374 under the fraudulent task order. Of this amount, $57,000 went to Dyer's wife. In addition, in 2001 and 2002 Dyer caused two other government contractors to employ his girlfriend as a graphic artist on contract work for the Navy. Dyer's girlfriend earned approximately $40,000 and kicked backed approximately $10,000 to Dyer.

On March 23, 2006, Dyer pled guilty to 12 felony counts, including conspiracy to present false claims, false claims, embezzlement of public money, and giving a gratuity to a public official. On June 29, 2006, Dyer was sentenced to 63 months in prison and was ordered to pay restitution of $81,344 and a special assessment fee of $1,200.

Four Individuals Involved in Identify Theft and Bank Fraud Pled Guilty

Treasury OIG worked jointly with other federal and state law enforcement agencies on an investigation of a complex bank fraud scheme wherein the participants created counterfeit checks by using names...and bank account numbers stolen from a number of victims….

Treasury OIG worked jointly with other federal and state law enforcement agencies on an investigation of a complex bank fraud scheme wherein the participants created counterfeit checks by using names, identification numbers, and bank account numbers stolen from a number of victims and used the routing codes assigned to six different financial institutions to legitimize

the checks. The checks were used to purchase a variety of merchandise, including jewelry, electronics, and furniture.

For his part in this scheme, John Caulder, of Richmond, VA, pled guilty in U.S. District Court for the Eastern District of Virginia on August 1, 2006, to conspiracy, bank fraud, and aggravated identity theft charges. Caulder faces up to 30 years imprisonment and a fine of up to $1 million for bank fraud, as well as a mandatory, consecutive 2-year prison term for aggravated identity theft. At the same time, Caulder's mother, Susan Caulder, also of Richmond, Virginia, pled guilty to obstruction of justice. Mrs. Caulder faces up to 20 years of imprisonment and a maximum fine of up to $250,000 when sentenced. In addition, Heather Nicole Weston and Katharine Caulder Staton – daughter of Susan Caulder – pled guilty to conspiracy to commit bank fraud and aggravated identity theft in July 2006. They will face the same penalties as John Caulder when they appear for sentencing scheduled in November 2006.

Mint Employee Sentenced for Embezzling Union Funds

An investigation by the Treasury OIG and the Department of Labor Office of Labor Management Standards revealed a scheme by Mary Garner, a Mint management analyst, to embezzle union dues. The investigation determined that Garner, who was also a labor union officer, misused her government travel card and attempted to charge the local union for travel expenses previously reimbursed by the government. The U.S. Attorney's Office for the District of Columbia reached a plea agreement with Garner who pled guilty to one count of mail fraud for her scheme to defraud American Federation of Government Employees Local 3656 of $12,195. Garner was sentenced on September 26, 2006, to 5 years probation, 6 months home detention, and 360 hours community service. She was also ordered to pay restitution of $11,959 with a special assessment fee of $100. Additionally, after the Mint proposed termination, Garner resigned.

Office of Technical Assistance Contract Employee Terminated

An OIG investigation revealed that an Office of Technical Assistance contract employee was aware of a reportable debt...and failed to disclose the debt on his public financial disclosure reports for years 2003 and 2004, as required under his contract with the Treasury.

An OIG investigation revealed that an Office of Technical Assistance (OTA) contract employee was aware of a reportable debt in the amount of $11,636 and failed to disclose the debt on his public financial disclosure reports for 2003 and 2004, as required under his contract with the Treasury. The contract employee, a former Special Agent with the Bureau of Alcohol, Tobacco and Firearms as well as the Environmental Protection Agency, worked as a Resident Advisor in Africa, advising on anti-public corruption matters. After initiation of the investigation, the employee's contract with OTA was terminated.

OCC Bank Examiners Suspended Without Pay for Accepting Gratuities from Bank Officials

An OIG investigation determined that eight OCC national bank examiners accepted gratuities (i.e., payment for meals and golf outings) from bank officials, in violation of OCC ethics policy and, potentially, 18 USC § 213 (acceptance of loan or gratuity by bank examiner). OIG found no evidence that the gratuities influenced the examiners in the performance of their official duties or that the examiners solicited or coerced the offering of a gift. OCC suspended without pay five examiners for 14 days, two examiners for 3 days, and one examiner for 1 day.

BPD Attorney-Advisor Suspended Without Pay for Misusing Government Equipment

An OIG investigation disclosed that a BPD attorney-advisor misused his government computer, Internet access and official time for inappropriate personal use, including viewing of sexually oriented and sexually explicit materials. In May 2006, BPD suspended the employee from duty without pay for 14 calendar days for using a government computer to access unauthorized sites of a sexual or inappropriate nature, and wasting government time.

BEP Employee Misused Government Travel Card

An OIG investigation determined that a BEP currency shipment checker/processor knowingly and without authority used his Citibank Government Travel Card to charge $6,108 in personal expenses. In addition, the employee failed to pay his monthly balances in full as required. As a result of the OIG investigation, BEP proposed termination of the employee. The employee resigned from his position effective August 23, 2006.

The following are updated cases of investigative activities from previous semiannual reports.

Correction of Erroneous Semiannual Reports: Former Treasury Acting CIO Sentenced for Making False Statement and Debarred, But Debarment Temporarily Enjoined

In our semiannual report for the period ended March 31, 2004, we stated that a former Treasury Acting Chief Information Officer, Maria "Mayi" Canales, agreed to plead guilty to a violation of 18 U.S.C. § 1018 for making false statements and to be debarred from doing business with the federal government for life. In our semiannual report for the period ended September 30, 2004, we reported that Ms. Canales had pled guilty; that she had been sentenced to probation, a fine, and community service; and that she had been debarred for life. These reports were incorrect in part. Ms. Canales did plead guilty to violating

18 U.S.C. § 1018 for making false statements to an OIG investigator, and was sentenced as reported. However, she had not agreed to be debarred for life, and in fact had not been debarred, at the time of the semiannual reports. It was not until June 27, 2006, that the Department debarred Ms. Canales from doing business with the federal government for a period of 3 years. On July 28, 2006, Ms. Canales brought suit in U.S. District Court for the District of Columbia against the Department and OIG, challenging the debarment and OIG's erroneous statements. As of September 30, 2006, the U.S. District Court has temporarily enjoined enforcement of the debarment, pending resolution of this challenge. OIG regrets its erroneous reporting on this matter.

Hamilton Bank Case

As previously reported, OIG, in conjunction with the Federal Deposit Insurance Corporation OIG, conducted an investigation that led to a 42-count indictment -- for conspiracy, wire fraud, securities fraud, false filings with the Securities and Exchange Commission, false statements to accountants, obstruction of examination of a financial institution, and making false statements to OCC -- against Eduardo Masferrer, former Chief Executive Officer of Hamilton Bancorp and Hamilton Bank (Hamilton), Juan Carlos Bernace, President and a Director of Hamilton, and John Jacobs, Senior Executive of Hamilton. They were indicted for their participation in a scheme whereby they fraudulently inflated the reported results of operations and financial condition of Hamilton and defrauded the investing public and the bank/securities regulators. In February 2005, Bernace pled guilty to two counts of securities fraud. In October 2005, Jacobs pled guilty to one count of securities fraud and one count of obstruction of an OCC examination.

Update: In May 2006, Masferrer was found guilty in the U.S. District Court for the Southern District of Florida for obstruction of an OCC examination, conspiracy, wire fraud, defrauding a financial institution, false statements, and securities fraud. On July 27, 2006, Masferrer was sentenced to 30 years incarceration, while Bernace and Jacobs were each sentenced to 28 months of incarceration.

Former BEP Employee Pleads Guilty to Theft of Currency from BEP

As previously reported, the Treasury OIG was notified by BEP Police of a possible theft of currency from the Western Currency Facility (WCF) in Ft. Worth, Texas. A joint investigation with the U.S. Secret Service identified a BEP employee, Donald Stokes, who was alleged to have removed at least $5,000 of $50 Federal Reserve Notes slated for destruction from the WCF. Further investigation disclosed that Stokes had been stealing currency, in the form of uncut notes, from the BEP facility since 1998. On July 13, 2005, Stokes pled guilty to one count of interstate transportation of stolen property for the $30,000 of currency that he admitted stealing from the WCF.

Update: On November 22, 2005, Stokes was sentenced to 41 months in jail and 36 months of probation. He was also ordered to pay a $10,000 fine.

OIG Participation in Baltimore Fraud Task Force Identity Theft Investigation Leads to Guilty Pleas and a Conviction

As reported in the previous semiannual report, OIG, as a member of the Baltimore Metropolitan Fraud Task Force, participated in an investigation that led to a 10-count indictment of an individual for bank fraud, aggravated identity theft, and aiding and abetting.

Update: The indictment charged Cleveland Kilgore with a scheme to defraud the Bank of America through unauthorized use, from September 2004 through March 2005, of the personal information of Bank of America account holders in California. Kilgore was charged with obtaining account holders' bank account numbers and balances, names, addresses, and driver's license numbers, and manufacturing identification for himself and two associates, Donna Spencer and Eric Wiggins. The scheme netted approximately $274,000 from Bank of America branch locations in Maryland, Virginia, North Carolina, and Florida.

On September 15, 2006, Eric Wiggins pled guilty to one count each of bank fraud, aggravated identity theft, and conspiracy. On September 19, 2006, Donna Spencer pled guilty to one count each of bank fraud and aggravated identity theft. On September 28, 2006, Kilgore was found guilty after a jury trial in the U.S. District Court for the District of Maryland on four counts of bank fraud, four counts of aggravated identity theft, and aiding and abetting. Wiggins is scheduled to be sentenced on December 11, 2006. Spencer's sentencing date is to be determined. Kilgore is scheduled to be sentenced on December 15, 2006.

BEP Supervisory Police Officer Misused Government Computer

As reported in the previous semiannual report, an OIG investigation determined that a BEP supervisory police officer used his assigned government computer to access pornographic Web sites on an almost daily basis and transmitted pornographic e-mails while on duty.

Update: As a result of the investigation, the BEP supervisory police officer received a 14-day suspension without pay.

Treasury OIG Hosts Delegation from China

On September 14, 2006, Inspector General **Harold Damelin**, Counsel to the IG **Rich Delmar**, Deputy Assistant Inspector General for Audit **Bob Taylor**, and Special Agent in Charge **Brian Crane** met with a delegation from the Ministry of Supervision, People's Republic of China, including Director General **Zhang Lijun**, Department of Personnel. We discussed the mission of U.S. government Inspectors General and the Treasury OIG. The meeting was arranged by the 21st Century Institute. The delegation also visited other federal agencies during its trip to Washington, DC. This was our second meeting with a delegation from the Ministry of Supervision; the first was in November 2004.

Chinese government officials are briefed by Inspector General Damelin and his senior staff on the mission of federal Offices of Inspector General.

Audit External Peer Reviews

Audit organizations that perform audits and attestation engagements of federal government programs and operations are required by *Government Auditing Standards* to undergo an external peer review every 3 years. The objective of an external peer review is to determine whether, during the period under review, the audit organization's internal quality control system is adequate and whether quality control policies and procedures are being complied with to provide the audit organization with reasonable assurance of conforming with applicable professional standards.

During this semiannual period, the Social Security Administration (SSA) OIG rendered an unqualified opinion on the Treasury OIG's system of quality control for the audit function for the year ended March 31, 2006. In its report dated August 18, 2006, SSA OIG also noted one finding in our system of audit quality control for which we have taken corrective action. The external peer review report is available on our website.

Also during this semiannual period, we completed an external peer review of the Department of Education OIG Office of Audit.

OTHER OIG ACCOMPLISHMENTS AND ACTIVITIES

OIG Participation in Forward Challenge 2006

On June 21, 2006, FEMA conducted a federal executive branch interagency exercise, Forward Challenge 2006 (FC 06), to test its readiness and capabilities to execute continuity of operations plans (COOP). FC 06 was a full-scale, externally evaluated, scenario-based exercise that gave each participating department and agency the opportunity to activate its COOP plan, deploy COOP personnel to an alternate site, and perform its essential functions from that alternate site. FC 06 provided a framework for testing the interoperability and interconnectivity between departments' and agencies' COOP sites to ensure compliance with the annual requirement outlined in Federal Preparedness Circular 65, *Federal Executive Branch Continuity of Operations (COOP)*, to engage in joint agency exercising of COOP plans. Treasury OIG participated in FC 06, providing integral support to Treasury's Emergency Management Center, as well as testing the OIG COOP.

IGATI Curriculum Review Board Update

The Inspectors General Auditor Training Institute (IGATI) was created by the President's Council on Integrity and Efficiency (PCIE) in December 1990 as a reimbursable program within Treasury OIG. IGATI provides training to enhance the skills, abilities, and knowledge of auditors in the federal OIG community. Under the leadership of Assistant Inspector General for Audit Marla Freedman, the IGATI Curriculum Review Board (Board) was formed in fiscal year 2005 to assist the PCIE Audit Committee in achieving its strategic goal to identify and provide useful, relevant, and cost-effective auditor training.

During this semiannual reporting period, the Board completed reviews of 4 IGATI courses, bringing to 11 the number of courses reviewed since the Board's inception. In brief, the Board reported that the 4 courses provided valuable training and also made a number of recommendations to further improve course content and delivery. Participating in the course reviews completed this period were the OIGs of the Departments of Defense, Interior, Commerce, U.S. Agency for International Development, Environment Protection Agency, and Social Security Administration.

In our last semiannual report, we discussed plans to consolidate IGATI with the Inspector General Criminal Investigator Academy and the Inspector General Management Institute to become the Inspector General Institute (IG Institute). During this semiannual period, the PCIE and Executive Council for Integrity and Efficiency (ECIE) decided to cancel the IG Institute initiative. In September 2006, the PCIE Audit Committee re-established IGATI with Treasury OIG as the cognizant agency. The PCIE Audit Committee will continue to have oversight over IGATI and has asked the Board to continue its assessments of course content and relevance.

OTHER OIG ACCOMPLISHMENTS AND ACTIVITIES

PCIE Awards

At the annual joint PCIE and ECIE awards ceremony on October 24, 2006, Treasury OIG received three Awards for Excellence in recognition of its work on certain audits completed during fiscal year 2006. An OIG special agent was also recognized in a multi-agency Award for Excellence. Additionally, Treasury OIG also accepted an Award for Excellence on behalf of a number of agencies participating in a PCIE-wide project.

The achievements recognized were as follows:

- An audit that found that the Treasury Communications Enterprise procurement was poorly planned, executed, and documented.
- An audit of BEP that identified an accounting issue having government-wide implications for increasing revenue to the Treasury General Fund.
- An audit of the major challenges faced by FinCEN to register money services businesses as required by the Money Laundering Suppression Act.
- A multi-agency civil investigation with Treasury OIG participation that resulted in millions of dollars in recovery for travel rebates related to government contracts that were improperly retained by several large public accounting and consulting firms.
- The exceptional support by the multi-agency IGATI Curriculum Review Board to further the PCIE Audit Committee's strategic goal for quality auditor training.

The PCIE and ECIE also bestowed its June Gibbs Brown Career Achievement Award posthumously to **William H. Pugh, III**, who served with the Treasury OIG for 10 years as the Deputy Assistant Inspector General for Financial Management and Information Technology Audit. Mr. Pugh was recognized for his exceptional service to both the Department of the Treasury and the Federal Audit Community. Our previous semiannual report was dedicated to the memory of Mr. Pugh, who passed away in February 2006.

Improper Payments Initiative

This Treasury OIG initiative directly supports the President's Management Agenda to reduce improper payments government-wide.

The Office of Investigations recently initiated, with the OIGs of five other agencies, a project to proactively identify potentially fraudulent benefit payments warranting further investigation. The other agencies we are working with on this initiative are the Department of Veterans Affairs, the Social Security Administration, the Railroad Retirement Board, the Office of Personnel Management, and the Defense Criminal Investigative Service. This Treasury OIG initiative directly supports the President's Management Agenda to reduce improper payments government-wide. Chief among our roles is to help federal agencies detect, investigate, and prevent criminal activity related to improper benefit payments, thus helping to ensure that taxpayer dollars are spent wisely

and efficiently. Since its inception in mid-July 2006, we have opened, in conjunction with the other participating OIGs, 20 investigative cases involving nearly $1.4 million in payments and made 3 arrests.

FECA Initiative

During the semiannual period, Treasury OIG special agents and auditors worked together to identify potential fraudulent activity within the FECA program at Treasury.

As reported in our semiannual report for the period ended March 31, 2006, we initiated a proactive project, which is being conducted jointly by the Offices of Investigations and Audit, to identify potential instances of fraud in the FECA program within Treasury. This project is part of a larger initiative being carried on throughout the Inspector General Community. Work on the project continued during this semiannual reporting period. Specifically, OIG special agents and auditors analyzed FECA payment and claim data for unusual items. As discussed on page 19 of this report, we determined one situation where FECA benefits continued to be paid after a BEP employee's death, and were received by the employee's daughter. OIG auditors are also assessing FECA program controls at selected Treasury bureaus.

Hurricane Katrina Fraud Task Force

On September 13, 2006, Attorney General Alberto R. Gonzales addressed the first annual conference of the Hurricane Katrina Fraud Task Force in New Orleans, LA. Assistant Attorney General Alice S. Fisher presented the Attorney General with the task force's first-year report. OIG participated in the gathering of more than 150 professionals to discuss trends and patterns in hurricane-related fraud, suggested best practices for law enforcement after future disasters, and task force accomplishments to date. The principal types of fraud on which the Task Force is now concentrating are government contract and procurement fraud, public corruption, government and private-sector fraud, identity theft, and fraudulent charities.

Among the cases highlighted in the annual report was OIG's investigation of Jeffrey Rothschild (described on page 18 of this report), which was successfully prosecuted by the U.S. Attorney for the District of Columbia.

Suspect activity should be reported to the Hurricane Katrina Fraud Task Force Hotline at (866) 720-5721, faxed to (225) 334-4707, or e-mailed to HKFTF@leo.gov.

Richmond, Virginia, Fraud and Identity Theft Task Force

As a member of the Metro-Richmond Fraud and Identity Theft Task Force, Treasury OIG is tasked to investigate criminal offenses involving advance fee and split-deposit schemes, counterfeit checks, Internet fraud, stolen government checks, and aggravated identity theft within the Richmond, Virginia, metropolitan area. The Assistant U.S. Attorney leading the task force is committed to aggressively investigating and prosecuting perpetrators of these

crimes. As discussed on page 20 of this report, OIG worked jointly with other task force members to investigate a complex bank fraud scheme involving four individuals who pled guilty during the period.

OIG Participation in the U.S. Secret Service–Sponsored Baltimore Fraud Task Force

Since joining the task force, OIG has played a part in the execution of 3 federal and state search warrants and participated in 11 arrests.

Since February 2006, OIG has actively participated in the U.S. Secret Service-sponsored Baltimore Fraud Task Force which includes agents and officers from a number of federal, state, and local law enforcement agencies in the Washington, DC and Maryland metropolitan areas. The primary objective of the task force is to combat large-scale fraud and identity theft that transcends jurisdictions or has a significant community impact. Our office's participation in the task force has involved OIG in a number of significant matters, including bank fraud investigations and crimes against Treasury, primarily concerning fraudulent transactions involving U.S. government checks issued by FMS.

Since joining the task force, OIG has played a part in the execution of 3 federal and state search warrants and participated in 11 arrests. As discussed on page 24 of this report, two individuals pled guilty and another individual was found guilty after a jury trial as a result of a task force investigation in which Treasury OIG participated.

OIG Participation in U.S. Secret Service–Sponsored DC Metro Area Fraud Task Force

As a result of OIG's participation in the task force, a number of significant investigations were referred to OIG…Additionally, OIG participated in the execution of 13 search warrants and 10 arrests.

OIG continued to be an active participant in the DC Metro Area Fraud Task Force, which is coordinated by the U.S. Secret Service, and includes agents and officers from a number of federal agencies and state and local departments from the metropolitan Washington, DC area. As a result of OIG's participation in the task force, a number of significant investigations were referred to OIG, including a significant Hurricane Katrina fraud case discussed on page 18 of this report involving over $100,000 in losses. Additionally, OIG participated in the execution of 13 search warrants and 10 arrests.

Treasury OIG Informs DC Metro Area Local Law Enforcement About Potential Frauds Involving False Treasury Instruments

The OIG takes seriously the misuse of the Treasury seal and other fraudulent Treasury instruments. Misuse of these instruments often involves identity theft that harm innocent victims. During 2006, we established contacts with 16 municipal and county law enforcement agencies in the DC Metro area to better inform them about potential fraudulent activities that involved the criminal or inappropriate misuse of Treasury seals or

fraudulent Treasury instruments, such as Uniform Commercial Code bills of exchange or bonds that appear to be Treasury instruments.

Summary of OIG Activity
For the 12 Months Ended September 30, 2006

OIG Activity	10/01/2005-03/31/2006	4/1/2006 – 9/30/2006	Period Totals
Office of General Counsel Activity			
Regulation and Legislation Reviews	3	15	18
Instances Where Information was Refused	0	0	0
Office of Audit Activities			
Reports Issued (Audits and Evaluations)	31	17	48
Disputed Audit Recommendations	0	0	0
Significant Revised Management Decisions	0	0	0
Management Decision in Which the IG Disagrees	0	0	0
Monetary Benefits (Audit)			
a) Questioned Costs	$0	$5,566,577	$5,566,577
b) Funds Put to Better Use	$0	$0	$0
c) Revenue Enhancements	$29,400,000	$0	$29,400,000
Total Monetary Benefits	$29,400,000	$5,566,577	$34,966,577
Office of Investigations Activities			
Reports of Investigation	16	13	29
Preliminary Inquiry Closing Memorandums	65*	39	104
Number of OIG Hotline Calls Processed	149	176	325
Allegations – Total Number Processed	210	278	488
Referrals Made During the Period	120*	185	305
Cases Open at Start of Period	183	177	183 Start
Cases Opened in the Reporting Period	40*	26	66
Cases Closed in the Reporting Period	46	22	68
Cases Open at the End of the Period	177*	181	181 End

STATISTICAL SUMMARY

OIG Activity	10/01/05-03/31/06	4/1/06 – 9/30/06	Period Totals
Inquiries Open at Start of Period	76	65	76 Start
Inquiries Closed in the Reporting Period	(42 + 5 conversions) 47*	(34 + 5 conversions) 39	(76 + 10 conversions) 86
Inquiries Opened in the Reporting Period	36	60	96
Inquiries Open at the End of the Period	65*	86	86 End
Judicial Actions			
Cases Referred for Prosecution	36*	28	64
Cases Accepted for Prosecution	10	15	25
Arrests	14*	21	35
Search Warrants	18	13	31
Indictments/Information	2*	2	4
Pleas	3*	12	15
Conviction by Trial	0	2	2
Imprisonment (Months)	83	479	562
Home Detention (Months)	0	6	6
Probation (Months)	72	60	132
Community Service (Hours)	0	360	360
Administrative Sanctions			
Adverse Personnel Actions	19*	10	29
Contractor Suspensions/Debarments	2*	0	2
Individual Suspensions/Debarments	1	0	1
Oversight Activities			
Quality Assessment Reviews	0	1	1
Management Implication Reports	0	0	0
Fraud and Integrity Briefings	11	6	17
Monetary Benefits			
Fines	$10,100	$1,300	$11,400
Restitution	$188,500	$140,497	$328,997
Recoveries	$0	$41,702	$41,702
Settlements	$384,795	$0	$384,795
Total Monetary Benefits	$583,395	$183,499	$766,894

*Numbers amended from the last reporting period, reflecting increases or decreases in data counts, are due to receipt of actions or changes after the reporting deadline.

Significant Unimplemented Recommendations

For Reports Issued Prior to September 30, 2005

Number	Date	Report Title and Recommendation Summary
OIG-02-015	9/02	*INFORMATION TECHNOLOGY: Treasury's Planning, Management, and Implementation of a Smart Card and Public Key Infrastructure (PKI) Needs Improvement* The CIO should ensure that Treasury: (1) establishes a Treasury program to effectively manage smart cards and PKI; (2) develops a program plan defining roles and responsibilities, and milestones and resources needed for smart card and PKI initiatives; (3) plans for adequate staffing of employees to support smart card and PKI infrastructure as enterprise architecture; (4) uses another hard token as an interim security measure along with smart cards to provide strong two-factor authentication for digital certificates; and (5) establishes appropriate record management controls for general, sensitive, and secret information related to the Treasury smart card and PKI infrastructure. (5 recommendations)
OIG-03-007	10/02	*INFORMATION TECHNOLOGY: Controls Over FinCEN's Law Enforcement Data Need Improvement* The FinCEN Director should establish a formal process for approving, transmitting, and maintaining system access authorization forms to reduce the risks associated with granting excessive or unauthorized access privileges, alterations, misunderstandings, and mishandled forms. (1 recommendation)
OIG-03-038	12/02	*PROTECTING THE PUBLIC: Treasury Departmental Offices' Control Over Computers Needs To Be Improved* DO should re-evaluate the method for reporting lost or stolen computers to ensure all losses are reported to the proper authorities. This should include periodic reconciliations between the CIO, Treasury Office of Security and Critical Infrastructure Protection, and the OIG Office of Investigations. (1 recommendation)
OIG-04-022	2/04	*Management Letter for Fiscal Year 2003 Audit of the Department of the Treasury Financial Statements* The Department should research and determine whether component reporting entities reporting on a basis other than Federal Generally Accepted Accounting Principles (GAAP) are required to do so by statute; that all reporting entities within the Department prepare their financial statements in accordance with Federal GAAP; and entities that are statutorily required to report on a basis of accounting other than Federal GAAP provide supplemental information in their annual reports that meets the reporting requirements of Federal GAAP, to include a Management Discussion and Analyses. (1 recommendation)

OIG-04-035	6/04	*GENERAL MANAGEMENT: Controls Over Security Need to be Improved at the Bureau of Engraving and Printing* The Bureau of Engraving and Printing Director should complete plans for its Integrated Security Systems and install its security upgrade systems expeditiously. (1 recommendation)
OIG-05-002	10/04	*MANUFACTURING OPERATIONS: Mint's Standard A-76 Competition Study for the Preparation of Ready-to-Coin Planchets Is Delayed and Requires Significant Action to Complete* The Mint Director should ensure that the required justification is prepared and the determination to provide or not provide Government Furnished Property is approved by the Assistant Secretary of Management and Chief Financial Officer. This should be accomplished before any future drafts of the performance work statement and the final solicitation are published. (1 recommendation)
OIG-05-032	3/05	*TERRORIST FINANCING/MONEY LAUNDERING: Office of Terrorist Financing and Financial Crimes Needs to Refine Measures for Its Performance Budget and Implement a Data Collection and Reporting System* The Assistant Secretary for Terrorist Financing should ensure that TFFC (1) implements the recently proposed performance measures, adjusted as appropriate based on planned discussions with OMB, and include the measures in the Department's fiscal year 2006 budget submission; (2) implements routine data collection and reporting procedures to help manage its operation and report on its performance measures; (3) creates a mechanism that will allow the office to regularly gather reliable data for organizations outside of Treasury; and (4) develops methods to assess the completeness and reliability of its performance measurement data. (4 recommendations)
OIG-05-035	4/05	*TBARR: Cost of Employee Move Delays During Main Treasury Building Renovation Could Not Be Determined* The Assistant Secretary for Management and Chief Financial Officer should implement procedures and maintain documentation supporting changes and accountability/responsibility for planned future moves associated with the Treasury Building and Annex Repair and Restoration (TBARR) Project. Such changes should be monitored to ensure that changes are appropriate and action taken as necessary so that the changes do not impact project completion and cost. Similar procedures and records should be maintained for any renovation of the Treasury Annex building, if funded. (1 recommendation)

OIG-05-043	8/05	*INFORMATION TECHNOLOGY: Effective Security Controls Needed to Mitigate Critical Vulnerabilities in Departmental Offices' Networked Information Systems* Due to the sensitive nature of the findings and recommendations, we designated the report Limited Official Use. Four recommendations in the report have not been implemented.

This list of OIG audit reports with unimplemented recommendations is based on information in Treasury's automated audit recommendation tracking system, which is maintained by Treasury management officials.

Summary of Instances Where Information Was Refused

April 1, 2006, through September 30, 2006

There were no such instances during this period.

Listing of Audit and Evaluation Reports Issued

April 1, 2006 through September 30, 2006

Financial Audits and Attestation Engagements

Report On Controls Placed In Operation and Tests of Operating Effectiveness for the Bureau of the Public Debt's Administrative Resource Center for the Period July 1, 2005 to June 30, 2006, OIG-06-035, 8/23/2006

Report on Controls Placed in Operation and Tests of Operating Effectiveness for the Bureau of the Public Debt's Trust Fund Management Branch for the Period August 1, 2005 to July 31, 2006, OIG-06-038, 9/13/2006

Report on Controls Placed in Operation and Tests of Operating Effectiveness for the Bureau of the Public Debt's Federal Investments Branch for the Period August 1, 2005 to July 31, 2006, OIG-06-039, 9/13/2006

Information Technology Audits and Evaluations

INFORMATION TECHNOLOGY: Effective Security Controls Needed to Mitigate Critical Vulnerabilities in the Office of the Comptroller of the Currency's Networked Information Systems, OIG-06-040, 9/14/2006 (Limited Official Use)

INFORMATION TECHNOLOGY: The OCC Disaster Recovery Exercise Was Successful, OIG-06-041, 9/19/2006 (Limited Official Use)

INFORMATION TECHNOLOGY: OCC Disaster Recovery Procedures Need to be Improved, OIG-06-042, 9/19/2006 (Limited Official Use)

INFORMATION TECHNOLOGY: Fiscal Year 2006 Evaluation of Treasury's FISMA Implementation for Its Intelligence Program, OIG-CA-06-004, 8/1/2006 (Classified)

INFORMATION TECHNOLOGY: Fiscal Year 2006 Evaluation of Treasury's FISMA Implementation for Its Non-Intelligence National Security Systems, OIG-CA-06-005, 9/26/2006 (Limited Official Use)

INFORMATION TECHNOLOGY: 2006 Evaluation of Treasury's FISMA Implementation, OIG-CA-06-008, 9/29/2006

Performance Audits

TERRORIST FINANCING/MONEY LAUNDERING: FinCEN Has Taken Steps to Better Analyze Bank Secrecy Act Data But Challenges Remain, OIG-06-030, 5/18/2006

FOREIGN ASSETS CONTROL: Assessing OCC's Examination of OFAC Compliance Was Hampered by Limited Documentation, OIG-06-033, 7/31/2006

BANK SECRECY ACT: OCC Did Not Take Formal Enforcement Action Against Wells Fargo Bank for Significant BSA Deficiencies, OIG-06-34, 8/18/2006

MANUFACTURING OPERATIONS: The Mint Needs to Determine Whether Its Long-Delayed A-76 Competition for Coin Blank Production Should Be Continued, OIG-06-036, 8/28/2006

REVENUE COLLECTION: TTB's Revenue Protection Audits Target the Largest Taxpayers, OIG-06-043, 9/26/2006

FOREIGN ASSETS CONTROL: Assessing OTS's Examination of OFAC Compliance Was Hampered by Limited Documentation, OIG-06-044, 9/26/2006

OCC: Allegations Regarding Supervision of National Family Bank, OIG-06-045, 9/27/2006

Supervised Contract Audits

CONTRACT AUDIT: Audit Report on Technical Graphics, Inc. Fixed Price Indefinite Delivery/Indefinite Quantity Proposal for NCD and NezGen Security Thread Substrate, Solicitation BEP-06-0001, OIG-06-037, 8/28/2006, **$5,566,577 Q**

Audit Reports Issued with Questioned Costs

April 1, 2006, through September 30, 2006

Category	Total		
	No. of Reports	Questioned Costs	Unsupported Costs
For which no management decision had been made by beginning of reporting period	0	0	0
Which were issued during the reporting period	1	$5,566,577	0
Subtotals	1	$5,566,577	0
For which a management decision was made during the reporting period	0	0	0
dollar value of disallowed costs	0	0	0
dollar value of costs not disallowed	0	0	0
For which no management decision had been made by the end of the reporting period	1	$5,566,577	0
For which no management decision was made within 6 months of issuance	0	0	0

The above audit was performed by the Defense Contract Audit Agency under our supervision. A "Questioned Cost" denotes that one or more of the following three situations exist: (1) an alleged violation of a provision of a law, regulation, contract, grant, cooperative agreement, other agreement or document governing the expenditure of funds; (2) a finding that, at the time of the audit, such cost is not supported by adequate documentation; or (3) a finding that the expenditure of funds for the intended purpose is unnecessary or unreasonable.

Audit Reports Issued with Recommendations that Funds be Put to Better Use

April 1, 2006, through September 30, 2006

At the beginning of the period, there were no audit reports from prior periods pending a management decision on recommendations that funds be put to better use. There were also no audit reports issued during this period with recommendations that funds be put to better use.

Previously Issued Audit Reports Pending Management Decisions (Over Six Months)

As of September 30, 2006

There are no audit reports issued before this semiannual reporting period that are pending a management decision.

STATISTICAL SUMMARY

Significant Revised Management Decisions
April 1, 2006, to September 30, 2006

There were no significant revised management decisions during the period.

Significant Disagreed Management Decisions
April 1, 2006, to September 30, 2006

There were no management decisions this period with which the Inspector General was in disagreement.

REFERENCE TO THE INSPECTOR GENERAL ACT

Reference	Requirement	Page
Section 4(a)(2)	Review of legislation and regulations	31
Section 5(a)(1)	Significant problems, abuses, and deficiencies	8-24
Section 5(a)(2)	Recommendations with respect to significant problems, abuses, and deficiencies	8-24
Section 5(a)(3)	Significant unimplemented recommendations described in previous semi-annual reports	33-35
Section 5(a)(4)	Matters referred to prosecutive authorities	32
Section 5(a)(5)	Summary of instances where information was refused	35
Section 5(a)(6)	List of audit reports	35-36
Section 5(a)(7)	Summary of significant reports	8-24
Section 5(a)(8)	Audit Reports with questioned costs	37
Section 5(a)(9)	Recommendations that funds be put to better use	37
Section 5(a)(10)	Summary of audit reports issued before the beginning of the reporting period for which no management decision has been made	37
Section 5(a)(11)	Significant revised management decisions made during the reporting period	38
Section 5(a)(12)	Management decisions with which the Inspector General is in disagreement	38
Section 5(a)(13)	Instances of unresolved FFMIA non-compliance	9
Section 5(d)	Serious or flagrant problems, abuses or deficiencies	N/A
Section 6(b)(2)	Report to Secretary when information or assistance is unreasonably refused	N/A

ACRONYMS

AML	Anti-Money Laundering
BAU	Blanking, Annealing, and Upsetting
BEP	Bureau of Engraving and Printing
Board	IGATI Curriculum Review Board
BPD	Bureau of the Public Debt
BSA	Bank Secrecy Act
CDFI Fund	Community Development Financial Institutions Fund
CFO	Chief Financial Officer
CIO	Chief Information Officer
COOP	Continuity of Operations
DC	District of Columbia
DO	Departmental Offices
DPW	Dubai Ports World
DRE	Disaster Recovery Exercise
ECIE	Executive Council on Integrity and Efficiency
ESF	Exchange Stabilization Fund
FBI	Federal Bureau of Investigation
FC 06	Forward Challenge 2006
FECA	Federal Employees' Compensation Act
FEMA	Federal Emergency Management Agency
FFB	Federal Financing Bank
FFMIA	Federal Financial Management Improvement Act of 1996
FinCEN	Financial Crimes Enforcement Network
FISMA	Federal Information Security Management Act of 2002
FMS	Financial Management Service
FTE	Full-Time Equivalent
GAAP	Generally Accepted Accounting Principles
GMRA	Government Management Reform Act of 1994
GSA	General Services Administration
Hamilton	Hamilton Bank
IG	Inspector General
IGATI	Inspectors General Auditor Training Institute
IPA	Independent Public Accountant
IRS	Internal Revenue Service
IRS-CI	IRS Criminal Investigation
MCA	Managerial Cost Accounting
Mint	United States Mint
MOU	Memorandum of Understanding
OCC	Office of the Comptroller of the Currency
OFAC	Office of Foreign Assets Control
OIA	Office of Intelligence and Analysis
OIG	Office of Inspector General
OMB	Office of Management and Budget
OTA	Office of Technical Assistance

ACRONYMS

OTS	Office of Thrift Supervision
PCIE	President's Council on Integrity and Efficiency
PKI	Public Key Infrastructure
PWS	Performance Work Statement
SAR	Suspicious Activity Report
SSA	Social Security Administration
TAD	Tax Audit Division
TBARR	Treasury Building and Annex Repair and Restoration
TCE	Treasury Communications Enterprise
TEOAF	Treasury Executive Office for Asset Forfeiture
TFF	Treasury Forfeiture Fund
TFFC	Office of Terrorist Financing and Financial Crime
TFI	Office of Terrorism and Financial Intelligence
TIGTA	Treasury Inspector General for Tax Administration
Treasury	Department of the Treasury
TTB	Alcohol and Tobacco Tax and Trade Bureau
USC	United States Code
WCF	Western Currency Facility
Web EFDS	Web-based Electronic Fund Detection System
Wells	Wells Fargo Bank
WSRC	Washington Supervision Review Committee

This Page Is Intentionally Left Blank

The Treasury Building in Washington, DC, is a National Historic Landmark, and has been located at the same site next to the White House since the federal government was moved from Philadelphia to the capital city in 1800. The current building began construction in 1836, replacing an earlier structure that had been destroyed by fire three years earlier. Architect Robert Mills designed the neo-classical building. As the Department of the Treasury expanded, the south, west, and north wings were added to the original Mills wing from 1855 to 1869. Pictured is a view of the Washington Monument from the south portico of the Treasury Building.

Source: Office of the Curator

contact us

Headquarters
Office of Inspector General
1500 Pennsylvania Avenue, N.W., Room 4436
Washington, D.C. 20220
Phone: (202) 622-1090;
Fax: (202) 622-2151

Office of Audit
740 15th Street, N.W., Suite 600
Washington, D.C. 20220
Phone: (202) 927-5400;
Fax: (202) 927-5379

Office of Investigations
740 15th Street, N.W., Suite 500
Washington, D.C. 20220
Phone: (202) 927-5260;
Fax: (202) 927-5421

Office of Counsel
740 15th Street, N.W., Suite 510
Washington, D.C. 20220
Phone: (202) 927-0650;
Fax: (202) 927-5418

Office of Management
740 15th Street, N.W., Suite 510
Washington, D.C. 20220
Phone: (202) 927-5200;
Fax: (202) 927-6492

Eastern Field Audit Office
408 Atlantic Avenue, Room 330
Boston, Massachusetts 02110-3350
Phone: (617) 223-8640;
Fax (617) 223-8651

Treasury OIG Hotline
Call Toll Free: 1.800.359.3898

Treasury OIG Web Page

OIG reports and other information are now available via the Internet. The address is http://www.treas.gov/offices/inspector-general