Semiannual Report To The Congress

April 1, 2004 – September 30, 2004

Office of Inspector General

Department of the Treasury

HIGHLIGHTS IN BRIEF

During this semiannual reporting period, our **Office of Audit** issued 18 audit and evaluation reports. The **Office of Investigations** work resulted in 6 successful prosecutions, 26 cases accepted for prosecution, $350,000 in settlements, and 5 adverse personnel actions against Treasury employees.

Some of the significant results from our work this period are described below:

- We issued two interim audit reports on our continuing audit of the Treasury Building and Annex Repair and Restoration (TBARR) Program. Congress mandated that we audit TBARR, which has received funding totaling $225 million through Fiscal Year 2004. We reported this period that, among other things, TBARR was not adequately planned at its inception; the original scope of the Main Treasury building renovation was amended numerous times resulting in delays and increased costs; ineffective management of employee moves to and from "swing space" during construction resulted in further delays and unnecessary costs; and there were various documentation problems with TBARR contract files.

- As a result of an investigation discussed in our prior Semiannual Report into the improper release of records, including classified information, the Department revised its policy concerning proper removal of documents by departing and former officials. Additionally, Treasury continued its efforts to develop a risk mitigation strategy that will involve future automated hardware and software changes, related process improvements, and technical training to prevent unauthorized releases of documents and information.

October 29, 2004

The Honorable John W. Snow
Secretary of the Treasury
Washington, DC 20220

Dear Mr. Secretary:

Following is our Semiannual Report to the Congress summarizing the activities of the Office of Inspector General for the 6-month period ending September 30, 2004. Fiscal Year 2004 represents the first full year of operations since Treasury's divestiture of most of its law enforcement functions to the Department of Homeland Security and the Department of Justice. The Department has successfully made the transition.

In our Fiscal Year 2003 Management Challenges letter, we identified the significant number of key leadership positions that were vacant in the Department as a significant management challenge. A number of those positions have been filled including the Deputy Secretary position. Deputy Secretary Bodman has begun to re-focus the Department on resolving its remaining material weaknesses, bringing more discipline to the budget process, and establishing more of a corporate management structure in the Department of the Treasury.

If the Department can maintain continuity of these initiatives, it has the opportunity to make significant progress on resolving longstanding material weaknesses. One of those weaknesses continues to be information security. As reported in our Fiscal Year 2004 Federal Information Security Management Act independent evaluation, Treasury's system inventory was not accurate, complete, or consistently reported. The number of systems reported by Treasury decreased from 708 in Fiscal Year 2003 to 237 in Fiscal Year 2004. Although Treasury reported that the number of systems certified and accredited increased from 24 to 85 percent, the major swings in inventory raise doubts as to the extent of real progress made. More effective management of information security will require clearer lines of authority and reporting between the Treasury bureaus and Treasury's Chief Information Officer (CIO). Treasury has taken a positive step in strengthening the role of the CIO by having that position report directly to the Deputy Secretary.

We remain committed to helping the Department improve controls and the efficiency of its operations. We will continue to focus our resources on Treasury's information security programs and the other major management challenges in the Department.

Sincerely,

Dennis S. Schindel
Acting Inspector General

This page intentionally left blank.

Table of Contents

This page is intentionally left blank.

Our Office

The Treasury's Office of Inspector General (OIG) was established pursuant to the 1988 amendment to the Inspector General Act of 1978, 5 USC Appendix 3. The OIG is headed by an Inspector General who is appointed by the President of the United States, with the advice and consent of the United States Senate. Serving with the Inspector General in the immediate office is a Deputy Inspector General. The OIG performs independent and objective reviews of Treasury programs and operations, except for 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 services related to the IRS.

The 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 (OA)** performs audits and evaluations. The Assistant Inspector General for Audit has two deputies. One deputy is primarily responsible for performance audits while the other deputy is primarily responsible for financial management and information technology audits. OA Headquarters is located in Washington, DC, and it maintains field audit offices in Boston and San Francisco.

The **Office of Investigations (OI)** performs investigations and conducts proactive initiatives that are aimed toward the detection and prevention of fraud, waste, and abuse in Treasury programs and operations. OI 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. OI headquarters and criminal investigative field staff are co-located in Washington, DC.

The **Counsel to the Inspector General** serves as the senior legal counsel and policy advisor to the Inspector General, Deputy Inspector General, and the Assistant Inspectors General. The Office of Counsel (OC) provides legal advice on issues that arise from statutorily mandated investigative, oversight, and audit activities performed by OA and OI. The OC also provides the OIG with legal advice related to government contracts, appropriations, budget formulation and execution, disclosure, records retention, tax information safeguards, equal employment opportunity, and personnel law. Additionally, OC represents the OIG in administrative proceedings before the Merit Systems Protection Board and the Equal Employment Opportunity Commission. Furthermore, the OC conducts the OIG's ethics training, financial disclosure, and Freedom of Information Act programs.

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, and reporting for the OIG. The Assistant Inspector General for Management is in charge of these functions.

OIG Values

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

About Treasury

The mission of the Department of the 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, the Treasury encompasses a wide range of programmatic and operational activities. Currently, approximately 107,500 people make up the Treasury. Of this workforce, the IRS has approximately 93,000 Full-time Equivalent (FTE) staff and the other Treasury bureaus and offices have approximately 14,500 FTEs.

Treasury Bureaus

Alcohol and Tobacco Tax and Trade Bureau (TTB) enforces and administers laws covering the production, use, and distribution of alcohol and tobacco products. TTB also collects excise taxes for firearms and ammunition.

Bureau of Engraving and Printing (BEP) manufactures paper currency, postage stamps, and other government documents.

Bureau of the Public Debt (BPD) manages U.S. Government borrowing, monitors the national debt, and processes bonds, notes, and T-Bill transactions.

Financial Crimes Enforcement Network (FinCEN) supports law enforcement investigative efforts against domestic and international financial crimes.

Financial Management Service (FMS) manages Federal government financial accounts.

Internal Revenue Service (IRS) collects income taxes and other forms of Federal revenue.

U.S. Mint (Mint) produces coins, medals, and coin-based consumer products.

Office of the Comptroller of the Currency (OCC) oversees and regulates all national banks and supervises the U.S. branches and agencies of foreign banks.

Office of Thrift Supervision (OTS) oversees and regulates all Federal- and many state-chartered thrift institutions.

Treasury Offices

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

Office of Terrorism and Financial Intelligence (TFI) develops and implements U.S. government strategies to combat terrorist financing domestically and internationally, and develops and implements the National Money Laundering Strategy as well as other policies and programs to fight financial crimes. Reporting to TFI are **FinCEN**, the **Office of Foreign Assets Control (OFAC)**, and the **Treasury Executive Office for Asset Forfeiture (TEOAF)**. 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. TEOAF manages the **Treasury Forfeiture Fund (TFF)**, which supports Treasury's national asset forfeiture program in a manner that results in Federal law enforcement's continued effective use of asset forfeiture as a law enforcement sanction to punish and deter criminal activity.

Office of International Affairs advises and assists in the formulation and execution of U.S. international economic and financial policy, including the development of policies with respect to 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) deals in gold and foreign exchange and other instruments of credit and securities as deemed necessary.

Community Development Financial Institutions Fund (CDFI Fund) expands the availability of credit, investment capital, and financial services in distressed 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 and meeting the financing requirements of the U.S. Postal Service.

Office of D.C. 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 (ATSB) issues 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.

Financial Management

Financial Audits

The Chief Financial Officer Act (CFO) 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 statements audits. The financial statements of certain other Treasury component entities are audited pursuant to other requirements, or due to their materiality to Treasury's financial statements. The OIG is also required to perform certain other financial related reviews. The Fiscal Year (FY) 2004 financial statement audits are currently in progress.

The following instances of non-compliance with the Federal Financial Management Improvement Act of 1996 (FFMIA) were reported in connection with the FY 2003 audits. The current status of these FFMIA non-compliances, including progress in implementing remediation plans, will be evaluated as part of our audit of Treasury's FY 2004 financial statements.

Entity	Condition	FY First Reported for FFMIA Purposes	Type of Non-Compliance
FMS	General control weaknesses may affect information in FMS system.	1997	Federal Financial Management Systems Requirements (FFMSR)
IRS	The general ledger does not conform to the U.S. Government Standard General Ledger.	1997	Standard General Ledger
IRS	IRS lacks an effective audit trail from its general ledger back to subsidiary detailed records and transaction source documents.	1997	FFMSR
IRS	Material weaknesses related to controls over unpaid tax assessments, tax revenue and refunds, and computer security.	1997	FFMSR, Federal Accounting Standards
IRS	IRS cannot rely solely on information from its general ledger to prepare financial statements.	1997	FFMSR
IRS	IRS lacks a subsidiary ledger for unpaid assessments.	1997	FFMSR

The table of the following page shows financial statement audit results for FY 2003 and FY 2002.

Treasury Audited Financial Statements and Related Audits

Entity	FY 2003 Audit Results			FY 2002 Audit Results		
	Opinion	Material Weaknesses	Other Reportable Conditions	Opinion	Material Weaknesses	Other Reportable Conditions
GMRA/CFO Requirements						
Treasury Department	UQ	2	1	UQ	4	0
IRS (A)	UQ	4	2	UQ	5	2
Other Required Audits						
BEP	UQ	0	0	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	0	0
OCC	UQ	0	2	UQ	0	1
OTS	UQ	0	0	UQ	0	0
TFF	UQ	0	1	UQ	0	1
Mint						
Financial Statements	UQ	0	0	UQ	1	2
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	0
Schedule of Loans Receivable	UQ	0	0	UQ	0	0
FMS						
Treasury Managed Accounts	UQ	0	0	UQ	0	0
Operating Cash of the Federal Government	UQ	1	0	UQ	2	0
TTB Schedule of Custodial Activities	UQ	0	3	N/A	N/A	N/A
International Assistance Programs	(B)	0	1	(B)	0	0

UQ Unqualified Opinion
N/A Schedule was not audited before FY 2003.
(A) Audited by the U.S. Government Accountability Office.
(B) Significant accounts of the International Assistance Programs were audited as part of the FY 2003 and FY 2002 Treasury Department consolidated financial statement audit. No separate audit reports were issued. These accounts were considered materially accurate.

The results of financial audits issued by our Office during this period that were performed in support of our audit of Treasury's FY 2003 consolidated financial statements are summarized as follows:

- An Independent Public Accountant (IPA), working under OIG supervision, rendered an unqualified opinion of **FMS**' FY 2003 and FY 2002 Schedules of Non-Entity Government-Wide Cash. The audit identified one material weakness, related to the ineffectiveness of computer controls, which was described in more detail in a separate, Limited Official Use (LOU) management letter. As noted in its comments to the auditor's report, FMS disagreed with this conclusion. The audit also identified an instance of reportable noncompliance with laws and regulations tested relating to OMB Circulars A-127 and A-130, which require controls to protect information. **(OIG-04-031, OIG-04-032 LOU)**

- An IPA, working under OIG supervision, rendered an unqualified opinion on **FMS**' FY 2003 and FY 2002 Schedules on Non-Entity Assets, Non-Entity Costs and Custodial Revenue. The audit did not identify any reportable conditions related to internal control or instances of reportable noncompliance with laws and regulations tested. The auditor also issued a separate LOU management letter describing certain electronic data processing internal control weaknesses that were noted during the audit. **(OIG-04-037, OIG-04-038 LOU)**

- An IPA, working under OIG supervision, rendered an unqualified opinion on the **Mint**'s FY 2003 and FY 2002 financial statements. The audit did not identify any reportable conditions related to internal control or any instances of reportable noncompliance with laws and regulations. **(OIG-04-033)**

Attestation Engagements

BPD Controls over the Processing of Transactions for Other Agencies

An IPA examined, under our supervision, the processing of transactions related to (1) accounting services provided to various federal government agencies by BPD's Administrative Resource Center Accounting Services Division (ARC-ASD), (2) transactions processing related to the investment accounts of various federal and state government agencies (Program Entities) maintained by the BPD's Trust Fund Management Branch (TFMB), and (3) transactions processing related to the investment accounts of various federal government agencies (Fund Agencies) maintained by the BPD's Federal Investments Branch (FIB). The IPA found: (1) BPD's description of controls for these activities fairly present controls that had been placed in operation as of June 30, 2004, for ARC-ASD and as of July 31, 2004, for TFMB and FIB; (2) except for a significant deficiency related to application software change controls noted for TFMB and FIB, these controls were suitably designed; and (3) controls tested by the IPA were effective during the period July 1, 2003, to June 30, 2004, for ARC-ASD and during the period October 1, 2003, to July 31, 2004, for TFMB and FIB. The IPA noted no instances of reportable noncompliance with laws and regulations for ARC-ASD and one instance of reportable noncompliance with laws and

regulations tested relating to OMB Circular A-130, which requires controls to protect information, for TFMB and FIB. **(OIG-04-040, OIG-04-041, OIG-04-042)**

Treasury Payments for DC Water and Sewer Services

The District of Columbia Public Works Act of 1954, as amended, requires federal agencies to make timely payments for DC water and sewer services. The Consolidated Appropriations Act of 2001 requires our office to submit a quarterly report to the House and Senate Committees on Appropriations analyzing the promptness of payments with respect to the water and sewer services furnished to Treasury by DC. For the third and fourth quarters of FY 2004, we found that the payments for these services were made promptly. **(OIG-04-030, OIG-04-036)**

Information Technology

Fiscal Year 2004 Independent Evaluation of Information Security for Treasury's Intelligence Program

As required by the Federal Information Security Management Act of 2002 (FISMA), we evaluated Treasury's information security program and practices as they relate to the Department's national security systems. Our classified report on this evaluation noted several weaknesses that warranted management's attention. **(OIG-CA-04-006 Classified)**

Controls Over Intelligence Sharing

We completed an evaluation, requested by the Treasury General Counsel, which found weaknesses in the automated process by which certain Treasury bureaus and offices obtained sensitive and classified intelligence information. **(OIG-CA-04-003 Classified)**

As discussed in our prior Semiannual Report, Inspector General Rush issued a "7-day letter" to Secretary Snow on February 3, 2004, that identified problems in the Department's handling of classified and other sensitive information. The results of the above evaluation and our FY 2003 FISMA evaluation of the Department's national security systems were cited in this letter.

Programs and Operations

Management of the Treasury Building and Annex Repair and Restoration Program (TBARR) Needs to Be Strengthened

After a June 1996 roof fire resulted in major damage to the Main Treasury building, Treasury decided to modernize the building. The Treasury Building and Annex Repair and Restoration (TBARR) Program was established in August 1998 for the purpose of (1) repairing and restoring the Main Treasury building to correct the damage caused by the

roof fire, (2) restoring the historic fabric of the building, and (3) modernizing the building and its systems to comply with current codes and standards. At the same time, the TBARR Program Office was established within the Office of Management to procure related services, oversee the design and construction activities, and coordinate employee moves during the construction. Starting with emergency funding received in FY 1996 for the fire damage, Treasury has received funding each year since, in accordance with no-year and multi-year spending plans. Through Fiscal Year 2004, Congress appropriated a total of $225 million for the TBARR Program.

The Conference Report (H.R. 108-401) for the Consolidated Appropriations Act, 2004, directed our office to audit all TBARR Program contracts since FY 1998. The audit is to include (1) a review of compliance with all applicable procurement laws, rules, and regulations, and the Architectural Barriers Act (ABA) of 1968, as amended; (2) a review of the scope, requirements, and cost reasonableness of the project, as well as the process for managing change orders to the original scope and design; and (3) a review of the effectiveness, efficiency, and economy of contractor operations. We are addressing these objectives in a series of audit reports.

During this semiannual period, we issued two Interim Audit Reports on the TBARR Program:

- As discussed in our August 9, 2004, Interim Audit Report, we found that: (1) the TBARR Program was not adequately planned at its inception; (2) the original scope of the Main Treasury building renovation was amended numerous times resulting in delays and increased costs; (3) ineffective management of employee moves to and from "swing space" during construction resulted in further delays and unnecessary costs; and (4) the TBARR Project Office accounting records, reconciliations, and reports were deficient.

- As discussed in our September 23, 2004, Interim Audit Report, we found that sampled TBARR contract awards substantially complied with federal procurement requirements and Treasury policy. However, the contract files did not always include required documentation supporting the type of contract used, documentation supporting the qualifications and designations of contracting officers' technical representatives (COTR) was incomplete and in some instances questionable, required interim and final evaluations of contractor performance were not documented in the contract files, and

action was not taken in a timely manner to close out completed contracts. We referred the instances of questionable COTR documentation to our Office of Investigations.

We also noted in this report that several key TBARR Program officials and other personnel had recently left federal service and expressed our concern that this loss of experienced personnel represents a significant risk to the successful completion of the TBARR Program activities within current anticipated timeframes and resources. To mitigate that risk, and considering that the President's FY 2005 Budget requested an additional $20.3 million for the TBARR Program, Treasury management needs to ensure qualified personnel are assigned to manage TBARR and to continually monitor the program.

Treasury management agreed with the findings in the two Interim Audit Reports and has taken or planned corrective actions that are responsive to our recommendations. **(OIG-04-039, OIG-04-043)**

We are continuing our audit of the TBARR Program to fully address the requirements of H.R. 108-401. Future planned work will include inspection of the renovation work, an assessment of contract and other costs charged to the TBARR appropriations accounts, and follow-up on the findings in our Interim Audit Reports.

Controls Over BEP Security Need to be Improved

We reviewed BEP's security function at its Western Currency Facility (WCF) in Ft. Worth, Texas, and its Washington, DC (Washington) facilities. BEP's security function is performed by police officers who are responsible for providing protection to the producer of the U.S. currency and other high value security items. The BEP police use electronic security systems that include controlled access, video surveillance, and a comprehensive system of alarms and intrusion detectors to secure and monitor the currency and other high value security items. Our review focused on BEP's security reporting structure, police training processes, and plans to update its security systems.

We found that: (1) BEP had a dual reporting structure for its physical security function for the WCF and Washington facilities and needed to better ensure consistency in its security program policies at both facilities; (2) police officers did not always meet firearms re-qualification requirements in a timely manner; (3) BEP's policy for training police officers was applied inconsistently between the WCF and the Washington facilities, and controls to ensure police officers received training were inadequate; and (4) certain weaknesses existed in BEP's security systems.

BEP agreed with our findings and has taken or planned corrective actions that were responsive to our recommendations for improving controls over security at both facilities. **(OIG-04-035 LOU)**

Compendium Report on Internal Control Weaknesses In Treasury Bureau Purchase Card Programs

The Government-wide purchase card program was established in 1989 to provide a low-cost, efficient means of obtaining goods and services directly from vendors. Purchase cards may only be used for official Government business and are primarily used for micro-purchases (purchases less than $2,500). In December 1993, Treasury directed all bureaus to begin using purchase cards for small purchases. Treasury issued Treasury Directive (TD) 76-04, *Government Purchase Card Program*, to provide bureaus guidance on the use of purchase cards. TD 76-04 requires the bureaus to establish approved uses and limitations on the types of purchases and spending limits. Using the Department's guidance, Treasury bureaus established additional guidance for employees. In 1998, Treasury selected *CitiBank* to provide all card services, including purchase cards, to its bureaus.

During the semiannual period, we issued a compendium report to Treasury management summarizing the results of prior OIG audits of purchase card programs at four bureaus—the Mint, FMS, OCC, and before it transferred to the Department of Homeland Security, the U.S. Customs Service. These bureau audits were completed between December 2002 and March 2004.

As discussed in the compendium report, we found internal control weaknesses in the purchase card programs at all four bureaus that often led to improper and questionable purchases. For example, at the Mint we found 15 improper split purchases (i.e. dividing a purchase into smaller amounts to get around the credit card limit) totaling over $100,000. Similarly, at FMS we found $7,900 in purchases of construction services that were purchased the same day but had been split into five transactions. We had also noted weaknesses in bureau policies and procedures, and a number of instances were these policies and procedures were not followed. While the improper and questionable purchases we observed did not involve large dollar amounts, we concluded that deviations from policies and procedures, coupled with a breakdown in internal controls, increased the risk of fraud, waste, and abuse.

We recommended that the Department's Office of the Procurement Executive reemphasize to all bureaus their responsibilities in managing the purchase card program; assess whether additional Departmental guidance was needed; and direct all bureaus to assess the adequacy of their policies, procedures, and internal controls, and implement changes as necessary to ensure compliance with Departmental guidance. Management agreed with the recommendations and planned to work with the bureaus and offices to improve their purchase card programs. **(OIG-04-034)**

Treasury's Rural Development Act Policy

As directed by the Consolidated Appropriations Act, 2004, we determined what policies and procedures are in place at Treasury Bureaus and Treasury Departmental Offices, excluding the IRS and TIGTA, to implement the Rural Development Act of 1972. In this regard, we noted that Treasury has a policy, TD 72-03, *Location of New Offices and Facilities in Rural Areas*, which gives first priority to the location of new offices and other facilities to rural areas. Four (4) of the 11 bureaus and offices we surveyed reported that they either established new offices, or renewed leases on a total of 29 facilities between January 1, 2003, to May 31, 2004. There were 14 new office locations. None of these facilities were located in a rural area, according to the respondents. These offices and other locations were added either under the considerations permitted in TD 72-03 to locate where either mission, service to customer, or safety/security of employees was critical to program operations, or were added to existing offices. The other 7 surveyed bureaus and offices reported no facility changes during the year. **(OIG-CA-04-005)**

Material Loss Reviews of Failed National Banks and Thrift Institutions

During the period, we issued a compendium report summarizing the results of the 7 Material Loss Reviews (MLRs) of failed financial institutions that our office performed between 1993 and 2002 pursuant to the Federal Deposit Insurance Corporation Improvement Act of 1991. Collectively, the current estimated amount of losses to the deposit insurance funds for these 7 failed institutions totals approximately $1.7 billion. We prepared this report to provide bank regulators, Treasury officials, congressional oversight committees, and other interested parties a historical perspective on: (1) the circumstances that led to the 7 failures resulting in material losses, (2) our observations on the supervision exercised by OCC or OTS over these institutions, and (3) our recommendations to improve supervisory policies and practices.

Deficient management at the institutions was the primary factor in the 7 failures. However, one institution—the First National Bank of Keystone (Keystone, West Virginia)—had an added dimension. Although management deficiencies were also evident at Keystone, fraudulent acts committed by the institution's management contributed to the institution's failure. For the 6 other failed institutions, management developed either new high-risk products/services or high-risk variations for existing business strategies and implemented them without appropriate safety and soundness standards. These business strategies were then aggressively pursued with little or no regard to the necessary management expertise, adequate oversight by the institutions' boards of directors, or adequate risk management strategies. Management at these institutions did not develop or implement adequate policies, procedures, or managerial expertise prior to engaging in higher-risk activities and, in some instances, were unresponsive to regulators' efforts to correct these unsafe and unsound practices.

With respect to OCC and OTS, we noted supervisory weaknesses in all 7 MLRs that included one or more of the following: (1) non-identification or attribution of the institutions' problems, (2) failure to review "red flags"; (3) failure to determine the institutions' true condition; (4) delayed supervisory response due to the institutions' apparent profitability; (5) failure to follow-up on past examination criticisms; and (6) failure to recommend, implement, or pursue more stringent enforcement actions.

The compendium report also listed the recommendations we made to OCC or OTS at the conclusion of each of the MLRs. In each case, OCC or OTS management concurred with the recommendations and instituted policies and procedures, expanded examination guidance, and took other corrective action that generally met the intent of our recommendations. **(OIG-CA-04-004)**

Missouri Federal Jury Finds Executives Guilty in Sinclair National Bank $3 Million Failure

As we reported previously (March 2004, p. 16), a grand jury in the Western District of Missouri returned a superseding indictment in November 2003 against Susan Sinclair Wintermute, the previous owner and director of Sinclair National Bank (SNB). Also charged as a co-conspirator was Clarence Stevens, the owner of Stevens Investment Corporation (SIC), who also serviced the $24 million in subprime loans he sold to SNB.

An extensive and complex joint federal criminal investigation – conducted by the Federal Deposit Insurance Corporation (FDIC) and Treasury OIGs, IRS Criminal Investigations Division, and the Federal Bureau of Investigation – disclosed Wintermute and Damian Sinclair, her then-husband (now deceased) who was co-owner of SNB and served as its chairman, acquired control of SNB in March 2000 after selling their Missouri financial services firm Sinclair Financial Group, Inc. (SFG) in October 1999. SNB would ultimately be closed by OCC and the FDIC-appointed receiver. SNB incurred $3 million in losses before filing for bankruptcy in 2001 which also left nearly 3,000 investors with more than $60 million in losses.

Wintermute and Sinclair submitted an application to the OCC in December 1999 to acquire control of the nationally chartered bank. Wintermute failed to disclose that she and Sinclair had been employed by Sinclair Management Services, Inc. (SMS) – a legal entity that owed SFG approximately $5 million. Also, Wintermute failed to disclose that she and Damian Sinclair were owed $5 million by SFG's owner as a result of their transfer of SFG to the new owner some two months earlier. SNB would eventually use insured depositor funds to purchase subprime consumer loan portfolios from SFG.

Unaware of all this activity, OCC approved the application to take control of SNB. Eventually, OCC's efforts were undermined when false documents were created and submitted to obstruct the bank examination process in an effort to cover up the prior false statements.

Following a 2-week trial brought by the U.S. Attorney for the Western District of Missouri and trial attorneys from the Fraud Section of the Justice Department's Criminal Division in August 2004, a federal jury found Wintermute guilty of conspiracy (18 U.S.C. § 371) to submit a false application and making a false statement (18 U.S.C. § 1001) in furtherance of the application submitted to OCC. Similarly, Stevens was convicted of conspiracy (18 U.S.C. § 371) to commit bank fraud. Both Sinclair and Stevens will be sentenced later

this year. Under the Federal Sentencing Guidelines, these bank executives face the possibility of 3 years in jail and fines.

Florida Federal Grand Jury Indicts Former Senior Executives of Hamilton Bank in $160 Million Failure

In June 2004, the U.S. Attorney for the Southern District of Florida announced the return of a 42-count indictment by the federal grand jury for false statements to accountants, obstruction of examination of a financial institution, and making false statements to OCC as well as conspiracy, wire fraud, securities fraud, and false filings with the Securities and Exchange Commission (SEC). In particular, a 2-year FDIC and Treasury OIG criminal investigation led to charges against three former senior executive officers of Hamilton Bancorp and Hamilton Bank, N.A. One executive also was charged with insider trading.

Hamilton Bancorp is a publicly-traded company in Miami-Dade County, Florida. It was the bank holding company and conducted operations principally through its wholly-owned subsidiary, Hamilton Bank, which was a trade finance bank in Miami-Dade County.

During 1998, Hamilton Bancorp had a market capitalization of more than $300 million. In September 1999, during the annual bank examination of Hamilton Bank, OCC bank examiners discovered questionable transactions in Hamilton's books regarding the bank's 1998 swap transaction involving the sale of Russian loans and the bank's purchase of Latin American and other non-Russian securities. By January 2002 OCC determined that Hamilton Bank had operated in an unsafe and unsound manner, closed the bank, and FDIC took receivership. Losses of approximately $160 million were incurred.

The three executives are alleged to have engaged in swap transactions (or adjusted price trades) to hide Hamilton Bank's losses (including $22 million-plus losses in 1998) and falsely accounted for the transactions to make it appear that no losses had been incurred. While the executives are alleged to have falsely reported the nature of the swap transactions to the investing public and OCC and SEC regulators, the indictment charged that internal tape-recordings were obtained which reflect that they openly discussed the transactions as swaps. Moreover, while this fraudulent activity was being concealed, one of the executives is charged with having engaged in illegal insider trading in Hamilton Bancorp's stock through the use of trust accounts.

In the end, these activities are believed to have unjustly enriched and benefited these executives through higher salaries, bonuses, and stock options, and would facilitate an upcoming registered securities offering to the investing public. One executive made nearly $2 million in bonuses, and other two executives each made more than $100,000 in bonuses while the fraud was concealed.

If convicted of conspiracy (18 U.S.C. § 371), obstruction of examination of a financial institution, (18 U.S.C. § 1517) or making a false statement (18 U.S.C. § 1001), the defendants face a statutory maximum term of 5 years imprisonment and a fine of up to $250,000 for each such count. If convicted of wire fraud, the defendants face a statutory maximum term of 30 years imprisonment and a fine of up to $1 million for each wire fraud count. If convicted of securities fraud, the defendants face a statutory maximum term of 10 years imprisonment and a fine of $1 million for each such count.

Treasury Contractor Resigns Following False Statement Investigation

Since 1990 Treasury's Office of Technical Assistance (OTA) has provided advisors to the former Soviet Union to assist in the transition from command to market economies. OTA's Financial Institutions Policy and Regulation Program (FIPRP) provides technical assistance to ministries of finance, central banks, deposit insurance agencies, problem bank resolution units, asset management and disposition divisions, and other banking related agencies or departments.

OTA notified Treasury OIG that it had contracted with an individual to be the Resident Tax Advisor (RTA) for the **Macedonia Minister of Finance**. Macedonia gained its independence from Yugoslavia and formed a parliamentary democracy in September 1991. While on deployment, OTA suspected the RTA provided false information (18 U.S.C. § 1001) on his application when it was disclosed he was disbarred from practicing law in the state of New York in January 2003. During our investigation, the RTA admitted he failed to inform OTA he had previously resigned from the New York Bar during an ongoing investigation by New York's Grievance Committee for the Ninth Judicial District for allegations of professional misconduct concerning breach of his fiduciary duty. The RTA's contract with OTA was valued at $809,000. The RTA received a total of $165,500 in salary during his contract performance until resignation. The OTA also expended approximately $5,500 in moving costs associated with the RTA. While pending a determination by the U.S. Attorney's Office for the District of Columbia (USAO-DC) with respect to whether it would seek prosecution, the RTA resigned from OTA in December 2003 resulting in the USAO-DC declining to pursue the matter further. The investigative results have been forwarded to the Department for potential suspension or debarment action.

Individual Pleads Guilty to Theft of Treasury Checks from FMS Contractor

Treasury's FMS disburses more than $1.7 trillion in federal payments annually – including Social Security, veterans' benefits, and income tax refunds – to more than 100 million people.

A joint criminal investigation – involving the Treasury and Department of Labor OIGs as well as the United States Secret Service (Secret Service) – resulted in a June 2004 guilty plea by Anthony Williams, a former government contractor employee, to eight counts of forgery in violation of 18 U.S.C. § 510(a)(2). His plea was in connection with an Eastern District of Pennsylvania Grand Jury indictment regarding his involvement in the theft and forgery of over 40 Treasury and private business checks valued at approximately $55,000.

Williams stole the checks while employed with an FMS mail sorting contractor. Sentencing is scheduled for Fall 2004.

$2.4 Million Predatory Lending Practice Under Investigation

In recent years the United States has seen a dramatic increase in a form of abusive conduct known as predatory lending. Predatory lending means imposing unfair and abusive loan terms on borrowers – often through aggressive sales tactics – that are designed to take advantage of borrowers' lack of understanding of extremely complicated transactions, and outright deception.

Predatory loans turn the dream of homeownership into a nightmare, in the worst instances ending in foreclosure. The damage done is increased by the fact that predatory loans are made in such concentrated volume in poor and minority neighborhoods where better loans are not readily available, and the loss of equity and foreclosure can devastate already fragile communities.

Predatory Lending Practices

- ⇒ Financing Excessive Fees into Loans
- ⇒ Charging Higher Interest Rates than a Borrower's Credit Warrants
- ⇒ Making Loans Without Regard to the Borrower's Ability to Pay
- ⇒ Prepayment Penalties
- ⇒ Loans for Over 100% Loan to Value
- ⇒ Yield-Spread Premiums
- ⇒ Home Improvement Scams
- ⇒ Single Premium Credit Insurance
- ⇒ Balloon Payments
- ⇒ Negative Amortization
- ⇒ Loan Flipping
- ⇒ Property Flipping
- ⇒ Aggressive and Deceptive Marketing - Live Checks in the Mail

Another scam involves the use of banking instruments known as "Bills of Exchange" (BOE). Similar to checks and promissory notes, BOEs can be drawn by individuals or banks and are generally transferable by endorsements. The difference between a promissory note and a BOE is that this product is transferable and can bind one party to pay a third party that was not involved in its

creation. If the BOEs are issued by a bank, they can be referred to as bank drafts. If they are issued by individuals, they can be referred to as trade drafts.

Joint criminal investigative efforts by Treasury OIG and the U.S. Department of Housing and Urban Development (HUD) OIG target predatory lending practices. Working with the U.S. Attorney for the District of Maryland, a federal search warrant was executed during May 2004 on an individual's residence and co-located business based on alleged violations of counterfeiting obligations of the United States (18 U.S.C. § 471), producing fictitious obligations of the United States (18 U.S.C. § 514), mail fraud (18 U.S.C. § 1341), bank fraud (18 U.S.C. § 1343), and conspiracy (18 U.S.C. § 371).

Approximately $2.4 million in BOEs are at the center of a fraudulent subprime loan scam. This individual's name is listed on an alleged private direct Treasury account with the Treasury Secretary registered as the trustee. An indictment is anticipated from the U.S. Attorney's Office, District of Maryland, in Fall 2004.

Former FMS Employee and Government Contractor Plead Guilty to Conspiracy, Wire Fraud, and Conflict of Interest Charges

As a follow-up to an indictment reported last period involving a former FMS employee and government contractor (March 2004, p. 16), the U.S. Attorney for the District of Maryland announced in September 2004 that Veronica Hardy-Everette and Charles Daniel Everette pled guilty to 1 count of conspiracy (18 U.S.C. § 371), 2 counts of wire fraud (18 U.S.C. § 1343), and 1 count of conflict of interest (18 U.S.C. § 207) and are scheduled to be sentenced in November 2004.

They now both face a maximum of 5 years in prison for each offense, followed by a term of supervised release of not more than 3 years, and a fine of $250,000. The court may also order restitution in the amount of $139,600 – to include the forfeiture of more than $65,000 in previously identified frozen assets. The investigative results have also been forwarded to the Department for potential suspension or debarment action.

Our investigation revealed that Hardy-Everette, a former FMS Employee Development Specialist (EDS), misused the procurement process to defraud the government of more than $139,600. In February 2004, a federal grand jury in Greenbelt, MD unsealed a 26-count indictment which alleged Hardy-Everette misused her official position from January 1999 to December 2000. During this period, Hardy-Everette worked in the training branch where she managed the disbursement of federal funds. As an EDS, she determined the training needs of employees and procured training services from private businesses. Hardy-Everette awarded 105 training agreements to Everette, her husband, and his businesses –Computer Image and C & D Training Consultants.

Senior Computer Specialist Pleads Guilty to Child Pornography Charge

Following our last report (March 2004, p. 15), the USAO-DC announced in July 2004 that Dennis Beheiter, a former FMS Senior Computer Specialist, was sentenced for the one count of possession of child pornography (18 U.S.C. § 2252) to which he previously pled guilty. The United States District Court imposed 27 months imprisonment and 3 years probation. Our investigation established that Beheiter used his government computer to download and collect child pornography. Forensic analysis revealed over 1,100 images of child pornography had been stored on his personal computer. He was terminated as an FMS employee losing 26 years vested towards federal retirement.

Former Acting Treasury CIO Sentenced for Making False Statement and Debarred for Life

In our March 2004 report (p. 15), we reported Treasury's former acting Chief Information Officer (CIO), Maya Canales, directed a consulting firm under contract with the Department to secure a $1.5 million subcontract with a company owned by the CIO's friend, as part of (or in exchange for), a $5.8 million contract that Treasury awarded to the consulting firm. The investigation revealed the acting CIO accepted various gratuities including jewelry and the use of a time-share rental property.

The former acting CIO pled guilty to making false statements in official certificates or writings (18 U.S.C. § 1018) and has been debarred for life from doing business with the federal government. In July 2004, the former acting CIO was sentenced in United States District Court to 1 year probation, fined $2,500, and ordered to perform 25 hours of community service.

U.S. Mint Account Technician Sentenced for Submitting False Travel Vouchers

As we reported previously (March 2004, p. 15), former Mint Account Technician, Shani Black, embezzled government funds by creating and submitting fraudulent travel vouchers. The investigation revealed that Black opened 5 bank accounts using various fictitious names. Further, she created, altered, and submitted 57 travel vouchers resulting in the unauthorized payment of $153,000 by means of Electronic Fund Transfers to the aforementioned bank accounts.

As a result of the investigation, Black pled guilty to making false statements (18 U.S.C. § 1001). In August 2004, she was sentenced to 12 months home detention/electronic monitoring, 5 years probation, and ordered to pay restitution of $153,471. We issued a Management Implication Report to the Mint in connection with our investigation to assist the bureau with addressing control weaknesses so as to prevent future submissions of false or fraudulent travel vouchers.

Businessman Indicted for Impersonating a Foreign Official and Misuse of Treasury Seal

In our March 2004 report (p. 16), we reported the arrest and indictment on federal charges of a businessman for federal charges related to the unauthorized use of the Treasury Seal (31 U.S.C. § 333) and forging the signature of a Treasury official (18 U.S.C. §712). Prior to the arrest, we executed a search warrant with support provided by the Secret Service, at the individual's Chicago residence. Secured were 86 boxes of evidence confirming his involvement in various criminal activities including the impersonation of a foreign government official (18 U.S.C. § 915), wire fraud (18 U.S.C. § 1343), forgery (18 U.S.C. § 510), and uttering counterfeit obligations and securities (18 U.S.C. § 472).

Included in the items recovered from the businessman's residence were 10,250 counterfeit U.S. Treasury Certificates of Deposit (CDs) – removing from the street CDs that would have allowed the individual and others to put "into play" bogus financial instruments having a purported combined worth of $5.3 trillion with which to facilitate their fraudulent scams. Acting upon our information, three associates of the businessman were arrested in Germany, England, and Canada by those nations' law enforcement agencies after it was disclosed that their victims had attempted to redeem some of the counterfeit CDs.

This investigation continues with additional federal charges expected involving mail fraud (18 U.S.C. § 1341) and bank fraud (18 U.S.C. § 1344). To date, monetary losses to U.S. victims, related to the advance fee schemes the subject has used, are in excess of $400,000. Additionally, there were over $500,000 in the forgery and uttering of altered and counterfeit checks. The case continues pending further investigation and judicial action with the U.S. Attorney for the Northern District of Illinois.

Operation Card Shark

As an active member of the multi-agency Secret Service **Metro Area Fraud Task Force** (MAFTF), Treasury OIG is an integral partner in the execution of "Operation Card Shark" (OCS). OCS targets the Adams Morgan area of Washington, DC, where criminal organizations are producing fictitious identification documents.

In one case, OCS members executed a federal search warrant resulting in 18 federal arrests at a residence where it was suspected a "Mill" had been established to produce fictitious identification documents. The 18 individuals who were arrested were all known to be involved in the conspiracy to produce and/or sell these bogus documents. Violations include fraud and related activity in

connection with identification documents and information (18 U.S.C. § 1028) and fraud and misuse of visas, permits, and other documents (18 U.S.C. § 1546).

At the time of this report, seized evidence is still being inventoried and assessed to ascertain whether any Treasury program or operation has been undermined by papers and/or documentation having been created, stolen, or illegally purchased.

Treasury OIG also provided MAFTF support on a case involving the execution of a federal search warrant in southeast Washington, DC. The related investigation involved the production of counterfeit United States currency. Among the evidence recovered, in addition to the computer, was a Hi-Point 9mm rifle with a 10-round magazine which had been "sawed off" and modified so that it was fully automatic.

MAFTF Partnership Results in Arrest of District Resident in Real Estate Scam Offering False Instrument Secured by the Secretary as Trustee

As we reported previously (March 2004, p. 17), our investigation of a DC resident involved his reported intent to defraud the Government (18 U.S.C. § 514) by presenting a falsely made and altered written instrument to a real estate company with the intent to purchase real property. The written instrument claimed that the Treasury Secretary was the trustee and that Muhammad possessed a private account in the amount of $470,422. Consequently, the subject was arrested and charged with allegedly uttering a worthless instrument under 22 DC Code, Section 3241, 3241(c).

Further investigation as part of the Secret Service MAFTF resulted in the execution of a search warrant at the subject's residence as well as an additional arrest warrant for the individual on charges of obstruction of justice (18 U.S.C. § 1510) and making threats against a federal officer (18 U.S.C. § 876). Evidence seized during the search warrant has implicated the subject's involvement in the aforementioned offenses. Judicial action is pending.

MAFTF Work Results in Conviction for Fraud against the U.S. Mint

An investigation conducted by Treasury OIG determined that a DC resident, Brett Streaty, engaged in a scheme to defraud the Treasury. Using worthless personal checks mailed to the Mint, Streaty received Mint products (coins). In addition, the Mint remitted the unfilled portion of his original order with Treasury checks which he negotiated.

The Treasury OIG and Secret Service MAFTF personnel executed an arrest warrant and recovered evidence that led to the USAO-DC charging Streaty with uttering worthless checks (18 U.S.C. § 510) to which he pled guilty and was sentenced to 180 days confinement, with 180 days suspended, and 2 years probation.

MAFTF Results in Arrest of Maryland Resident for Bank Fraud and Forgery

In August 2004, Treasury OIG and Secret Service MAFTF personnel arrested a Maryland resident for bank fraud (18 U.S.C. § 1344), forging endorsements on Treasury Checks, (18 U.S.C. § 510), and uttering counterfeit obligations of the United States (18 U.S.C. § 472). It is alleged that the individual attempted to defraud a federally insured bank by depositing an altered Treasury Check in the amount of $91,018 into a personal bank account belonging to her mother. The U.S. Postal Inspection Service has joined this Secret Service MAFTF investigation to assess suspicious activity involving altered and fraudulent U.S. Postal Money Orders (18 U.S.C. § 500) with losses exceeding $50,000.

Richmond Task Force Partnership Results in Arrest of Women for Robbery of a Treasury Check from a U.S. Mail Carrier

A joint Treasury OIG and U.S. Postal Inspection Service investigation, working together with the Richmond, VA, Task Force, resulted in the arrest of a Richmond resident on charges stemming from robbery "by force" of a U.S. Mail Carrier. During the robbery, it is alleged that a Treasury Check for $1,203 was stolen, subsequently forged, and uttered by the subject for her personal gain. Additional investigative work continues to assess the subject's background with respect to her involvement in other criminal activity.

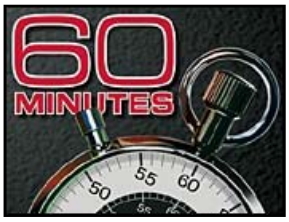
Virginia Couple Arrested on Credit Card Fraud and Identity Theft Charges

In August 2004, the Treasury OIG, U.S. Postal Inspection Service, and the Federal Bureau of Investigation (FBI) executed a federal search warrant on the residence of a suspect couple located in Richmond, VA. The search warrant related to an ongoing federal investigation involving identity theft and over $800,000 in bank fraud and credit card fraud that led to the purchase and resale of $2.5 million in cigarettes.

During the execution of the search warrant, federal arrest warrants were served on the couple charging each of them with one count of mail fraud (18 U.S.C. § 1341), bank fraud (18 U.S.C. § 1344), identity theft (18 U.S.C. § 1028), and illegal use of a social security number (42 U.S.C. § 407). Both subjects were held on immigration violations pending their appearance before the U.S. District Court in the Eastern District of Virginia.

Classified and Sensitive Treasury Documents Compromised After Improper Release to Former Treasury Secretary

As previously reported (March 2004, p. 18), we issued a Management Implication Report (MIR) to assist Treasury in addressing systemic weaknesses that contributed to the improper release of records, including classified information, to former Secretary O'Neill.



Treasury has since taken significant corrective actions to address these weaknesses. Included among the short-term remedial measures, taken in response to our MIR, are: (1) completion of security training for all DO employees; (2) hiring a Deputy Assistant Secretary for Security to develop a comprehensive security training program which elevates and institutionalizes overall security awareness levels within the Department; (3) completion of a risk-based review of the documents in question to mitigate if not negate the likelihood of further compromise; and (4) restoration of the affected systems.

Strategically, Treasury continues to develop a risk mitigation strategy that will involve future automated hardware and software changes, related process improvements, and technical training to prevent another incident. Operationally, the Department's General Counsel has forwarded a final draft Treasury Order to the Secretary which, when implemented, will provide a framework within which the removal of documents by departing and former officials will now be properly administered.

Director Suspended for Operating a Personal Business

An allegation was received indicating a BPD Division Director was misusing government property to perform work which supported his personal business activities while on official duty. Our investigation confirmed the Director did not obtain prior written approval before engaging in outside employment or business activity. In fact, he spent many hours at work misusing a BPD computer, government software, and related printing equipment to design home improvement plans for which he most recently charged his personal customers $1,500. Upon further review, it was found that the Director also filed a false Office of Government Ethics Form 450 Confidential Financial Disclosure Report by failing to disclose his personal business activities as well as related income. While the Department of Justice declined to criminally prosecute the matter, it was referred to BPD for administrative disciplinary action as his conduct also violated the Standards of Ethical Conduct for Employees of the Executive Branch (5 C.F.R. Part 2635) and Treasury Supplemental Standards (5 C.F.R. Part 3101). In addition to receiving a 14-day suspension from duty without pay, the matter has been referred to the IRS for further audit of individual and/or business tax documentation.

Government Employee Admits Carrying a Handgun while on Official Duty

In June 2004, an OCC Associate National Bank Examiner resigned from employment after admitting to having violated Treasury Employee Rules of Conduct. Our investigation confirmed the employee, legally registered as the owner of a .22 caliber pistol, improperly carried the firearm while on official travel to and from government-related work assignments.

Contractor Agrees to Pay $350,000 to Settle Justice Department Civil Fraud Litigation

In March 1997, Treasury's BEP entered into a five-year, $5 million contract with Chemical & Engineering Services (C&E) in Vienna, VA. C&E, a subsidiary of Ashland Chemical Company (Boonton, NJ) doing business as Drew Industrial Corporation (Drew), was hired to provide the chemically-based water treatment services necessary for BEP to cool high-speed, sheet-fed rotary presses and power plant operations.

A joint investigation by Treasury OIG, General Services Administration (GSA), and the Defense Criminal Investigative Service revealed contract irregularities between C&E and Drew indicating BEP had been over-charged for these services – by as much as 51 percent or more than $76,000 between 1997 and 2000. As of September 2004, in the Eastern District of Virginia, Drew agreed to pay the government $350,000, without admitting fault or liability, to settle civil litigation alleging a scheme by C&E and Drew to defraud BEP through use of a GSA Multiple Award Schedule that sold their products to the government at a higher price than their commercial customers.

Office of Audit

Acting Inspector General Testifies on Bank Secrecy Act (BSA) and Foreign Sanctions Program

On June 16, 2004, Acting Inspector General Schindel testified before the Subcommittee on Oversight and Investigations of the House Committee on Financial Services in its hearing on *Oversight of the Department of the Treasury*. Also testifying at this hearing were the Deputy Secretary of the Treasury, the Director of FinCEN, the Director of the OFAC, and the Chief of Criminal Investigation, IRS. As requested by the Committee Chairwoman, the topics covered in Mr. Schindel's testimony were: (1) our findings on BSA compliance efforts at OCC, OTS, IRS, and other regulators; (2) our opinions on OCC and OTS oversight of BSA compliance by banks in their private banking and trust operations; (3) whether the FinCEN database can be used efficiently by other agencies; and (4) any concerns resulting from our review of the OFAC foreign sanctions program.

In the testimony, Mr. Schindel informed the Subcommittee that our office's oversight of Treasury's role in combating terrorist financing, money laundering and other financial crimes was among our highest priority work. In this regard, we designated it as 1 of Treasury's 6 most significant management challenges. Mr. Schindel noted that while Treasury takes its BSA responsibilities seriously, in almost every area we have audited we have identified problems significant enough to impact Treasury's ability to effectively carry out its role in combating terrorist financing and money laundering. With regard to the Subcommittee's topics, Mr. Schindel highlighted the following past work by our office:

- In January 2000, we reported that OCC needed to improve its BSA compliance exams. Specifically, we found that many of the exams in our sample lacked sufficient depth to adequately assess a bank's compliance, OCC rarely referred BSA violations to FinCEN, and OCC procedures did not require examiners to review suspicious activity reports (SAR) filed by examined banks.

- In September 2003, we issued a report on BSA enforcement actions at OTS. We found that OTS was not aggressive in taking enforcement actions against thrifts in substantial non-compliance with BSA requirements.

- In November 2001, we completed an audit of OCC's oversight of BSA compliance in private banking and trust operations. We found that OCC needed to focus greater attention on private banking and trust operations when conducting BSA compliance exams. In 60 percent of the exams we tested, OCC examiners did not cover the bank's private banking operations; where OCC did include private banking or trust

operations in its BSA compliance exams, the exams often lacked sufficient testing of high risk transactions commonly associated with money laundering.

- We completed two audits on the accuracy and reliability of the FinCEN BSA database for Suspicious Activity Report (SAR), and we have one in process. These audits have consistently shown that the SAR database lacked critical information, included inaccurate information, or contained duplicate SARs.

- In October 2002, we issued an audit report on FinCEN's efforts to deter and detect money laundering in casinos and its related enforcement actions. IRS is responsible for BSA compliance examinations of casinos; we found that FinCEN was inconsistent and untimely in its enforcement actions against casinos for BSA violations referred by IRS.

- In April 2002, we reported that the Office of Foreign Asset Control (OFAC) was limited in its ability to directly monitor financial institution compliance with foreign sanction requirements. Like FinCEN, OFAC is dependent on other regulators to examine for compliance, and our testing found gaps in the regulators' examination coverage.

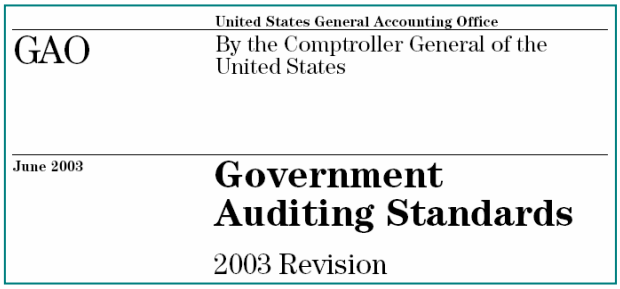
Mr. Schindel concluded his testimony with several observations. One, while the BSA compliance process is dependent on many federal and non-federal regulators, ultimately it is Treasury's responsibility, primarily through FinCEN, to ensure that there is adequate compliance and law enforcement is getting what they need. In this regard Treasury could do a better job. Second, the universe of BSA filers is expanding. This will result in dispersing BSA compliance monitoring among even more regulatory bodies. One of FinCEN's challenges has been ensuring that the regulators of these various BSA filers provide adequate and effective BSA compliance monitoring. To this end, FinCEN's approach has been focused on consensus building rather than leading, an approach that has met with limited success. For the current regulatory structure to work, it must be effectively managed through a cohesive effort that transcends the stovepipes of the individual regulators. FinCEN needs to take a more aggressive leadership role in that effort and require from all those involved in the regulatory structure an approach that, while risk-based, is thorough and intolerant of noncompliance. FinCEN also needs to be more engaged in analyzing the results produced by the various regulators so that it can be more proactive in addressing gaps in compliance monitoring.

Mr. Schindel also noted that this type of approach would apply to programs for which OFAC is responsible as well since it also relies on other regulators to administer its programs. The newly created Treasury Office of Terrorism and Financial Intelligence, to which FinCEN and OFAC report, can be the vehicle to pull this all together and establish a regulatory structure for BSA and OFAC sanction programs that is strong, effective, and accountable.

Top Treasury Officials Briefed on OIG Reviews of the BSA and Foreign Sanctions Program

During the period, we briefed newly appointed Treasury officials on our past, ongoing, and planned audits of Treasury's administration of the BSA and foreign sanctions programs. These officials included Deputy Secretary of the Treasury Samuel Bodman, Under Secretary for Enforcement Stuart Levey, and FinCEN Director William Fox. Our past work is summarized as part of the above discussion of the Acting Inspector General's recent congressional testimony.

External Quality Control Review



Audit organizations that perform audits of federal government programs and operations are required by *Government Auditing Standards* to undergo an external quality control review every 3 years. The objective of a quality control review is to determine whether the organization's internal quality control system is in place and operating effectively to provide reasonable assurance that established policies and procedures and applicable auditing standards are being followed.

During this semiannual period, the National Aeronautics and Space Administration (NASA) OIG rendered an unqualified opinion on the Treasury OIG Office of Audit's system of audit quality control for the period ended March 31, 2003. In a letter dated August 2, 2004, NASA OIG also noted 11 reportable conditions in our system of audit quality control for which we have taken or planned corrective action. The external quality control review report is available on our website.

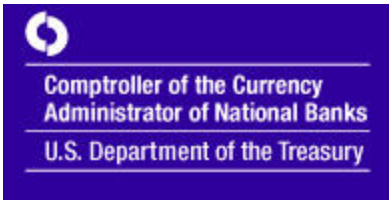
OIG Presentations Before Professional Associations and Treasury Conferences

The OIG continues to promote improved management and accountability within the Department and throughout the Federal government. Office of Audit representatives serve on professional and governmental task forces and committees, and have made numerous presentations on Federal financial management, auditing, and information security issues. Recent speaking engagements have included presentations by **Bill Pugh**, Deputy Assistant Inspector General for Financial Management and IT Audits, at the 2004 American Institute of Certified Public Accountants' National Governmental Accounting and Auditing Update Conference, the 2004 Association of Government Accountants Professional Development

Conference, and the annual Treasury Chief Financial Officers Symposium, and by **Joey Maranto**, IT Audit Manager, at the annual Treasury Chief Information Officers Symposium.

Office of Investigations

Jurisdictional Dispute with OCC



In our last Semi-Annual Report, we reported that we had sought information from OCC in connection with an investigation involving a failed bank. OCC questioned the OIG's jurisdiction, and refused to provide information. The OIG brought this matter to the Secretary's attention, pursuant to Inspector General Act § 6(b) (2), as well as to House and Senate oversight committees.

In the last 6 months, other instances of non-cooperation have occurred, involving, for example, OCC's oversight lapses regarding Riggs Bank, and the activities of a former OCC Examiner in Charge who accepted a position with Riggs Bank. After discussions between the Comptroller of the Currency and the Acting Inspector General, the OCC did promise cooperation with OIG investigators.

The OIG has pressed its position that it has jurisdiction to investigate external parties when there are threats to the integrity of a Departmental program or operation, for example efforts by banks to corrupt or impede OCC's bank examination and oversight functions.

The Department asked the OIG and OCC to present their arguments on this expanding issue of OIG jurisdiction to the General Counsel for his evaluation and resolution. At this time, the Office of General Counsel is reviewing arguments presented by the OIG and OCC.

President Praises Treasury Secretary for Identity Theft Work

Identity theft is the fastest growing financial crime in America. It affects some ten million people a year, removes some $50 billion out of the U.S. economy, and has a wrenching affect upon the lives of the people affected.

Credit underlies our system of commerce. People need to have confidence that when they get a credit card, when they use credit, when they go into the consumer credit markets, their identity isn't going to be stolen. And if they are at risk of their identity being stolen, they are going to be a lot less willing to engage in the commerce using credit. By, combating identity theft and fraud, we restore confidence in our credit institutions because this type of crime is a real threat to our credit system and the way our credit markets operate.

Frequently, the following question is asked, "What exactly is identity theft and identity fraud?" The simple answer, both are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception – typically for economic gain.

This problem became so pervasive in the 20th century that by 1998, Congress passed the Identity Theft and Assumption Deterrence Act. Created was the new federal offense of identity theft prohibited acts, (18 U.S.C. § 1028). Nearly 6 years later, however, the challenge of combating identity theft and identity fraud remains.

In an effort to give criminal investigators and prosecutors the necessary tools to create a credible deterrence against these crimes, in July 2004, at a press conference held by the President, he took time to acknowledge the leadership of both the Secretary of the Treasury and the Attorney General for their work that led to the passage of the ***Identity Theft Penalty Enhancement Act***. Proscribing prison sentences for those who use identity theft to commit other crimes, including terrorism, a new federal offense of ***aggravated identity theft*** now exists on the books.

These punishments come on top of any punishment for crimes that proceed from identity theft. For example, when someone is convicted of mail fraud in a case involving stolen personal information, judges now impose two sentences, one for mail fraud, and one for aggravated identity theft. Those convicted of aggravated identity theft must serve an additional mandatory 2-year prison term. Someone convicted of aggravated identity theft, such as using a false passport in connection with a terrorism case, would receive an additional prison sentence of 5 years. In addition, judges will not be allowed to let those convicted of aggravated identity theft serve their sentence on probation.

While external parties remain the most prevalent threat, ***the federal government's most significant identity theft vulnerability is the criminal conduct which emanates from within*** – those employees or contractors inside government who, either acting alone or in conspiracy with another, choose to abuse the public's trust by stealing or misusing a person's identity and/or related personal identification number (PIN). Sharing concurrent responsibility with the FBI for ***fraud and other crimes*** within the federal government, the IG community plays a most significant role in helping to not only detect or identify identity theft or identity fraud, but to prevent or deter it from occurring in the first place. As the President recently noted:

> "Most importantly, this law also raises the ***standard of conduct*** for people who have access to personal records through their work at banks, ***government agencies***, insurance companies, and other storehouses of financial data."

In February 2003, the Social Security Administration (SSA) IG issued a report to the ***President's Council on Integrity and Efficiency*** (PCIE) entitled *Federal Agencies' Controls over the Access, Disclosure and use of Social Security Numbers by External Entities*. This report served to follow-up on a Government Accountability Office (GAO) study and provided a more in-depth analysis of federal agencies' Social Security Number (SSN) controls related to contractor access, databases, non-Government access, and disclosure. The conclusion of the PCIE report reads as follows:

> "Some Federal agencies are at-risk for improper access, disclosure and use of SSNs by external parties, despite safeguards to prevent such activity. We recognize that Federal agencies' efforts cannot eliminate the potential that unscrupulous individuals may inappropriately acquire and misuse SSNs. Nonetheless, we believe each Federal agency has a duty to safeguard the integrity of SSNs by reducing opportunities for external parties [and our own employees] to improperly obtain and misuse the SSNs. Given the potential risk for individuals to engage in such activity, we believe Federal agencies would benefit by strengthening some of their controls over the access, disclosure and use of SSNs by external entities." (p. 7)

For example, Treasury's FMS effects more than 240 million payments disbursing $1.7 trillion to more than 100 million individuals for their social security and veterans' benefits, income tax refunds and other federal payments. In addition to an SSN, PINs include employee identification numbers and other individual identifiers that agencies assign. As of January 2004, FMS was slated to remove the use of PINs from 98 percent or 235.2 million payments issued on behalf of all federal agencies. As we look ahead to FY 2005, Treasury OIG will work closely with our law enforcement partners and the Department's programs and operations, like FMS (i.e., 4.8 million remaining recipients targeted for elimination by 2005), to remove or significantly minimize any remaining vulnerabilities.

PCIE IT Roundtable – Investigations Working Group Activity

The PCIE Information Technology Roundtable's mission is to facilitate effective information technology (IT) audits, evaluations, and investigations by Inspectors General, and to provide a vehicle for the expression of the IG community's perspective on Government-wide IT operations.

In FY 2004, Treasury OIG, working in partnership with the U.S. Department of Education OIG, met with the larger federal law enforcement community membership to address the investigation of, and delivery of critical infrastructure protection related to, cybercrimes as well as network intrusion detection and prevention activities. In particular, the role OIG criminal investigators will play in supporting their departments or agencies within the context of the lead responsibilities of the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) given the divestiture of the National Infrastructure Protection Center (NIPC) from the FBI to DHS. The Secret Service, which shares concurrent responsibility for cybercrimes with the FBI, has detailed personnel to lead the

NCSD. Discussions included OIG criminal investigator detailees to the NCSD and agreements establishing task force-like working protocols.

Given our concurrent investigative responsibilities with the FBI and others on the investigation of fraud and other crimes against and within the Department's programs and operations, the PCIE IT Investigations Working Group will continue to provide a forum to collaborate not only with law enforcement and other OIG personnel, but colleagues in the IT field (including the federal CIOs and staff, security professionals, and members of the Executive Council on Integrity and Efficiency). We will promote effective teamwork in addressing Government-wide initiatives, improving OIG IT activities, and safeguarding national IT assets and infrastructure. Finally, we will conduct relevant IT educational and training activities, advise the PCIE on IT issues, and provide for IT information exchange among the OIG's, including best practices and current capabilities.

International Loan and Grant Fraud – Treasury OIG Meets with Senate Foreign Relations Committee Staff

Treasury's mission is to promote the conditions for prosperity and stability in the U.S. and encourage prosperity and stability in the rest of the world. The objective of the Department's Office of International Affairs (OIA) is to increase economic growth and improve economic stability in developing countries, emerging market countries, and industrial countries.

U.S. Senate Committee on Foreign Relations

Since 1960, Congress has appropriated $39 billion to fund the Multilateral Development Banks (MDBs) – the Inter-American Development Bank (IADB), African Development Bank (AfDB), Asian Development Bank (AsDB), and European Bank for Reconstruction and Development (EBRD). OIA provides oversight of the U.S. Government's participation in the International Monetary Fund (IMF) and the MDBs. The Senate Committee on Foreign Relations has an oversight role regarding of Treasury's activities in this area.

Fraud and corruption in MDB funded programs and operations remain a significant concern. In FY 2004 the Committee held hearings entitled *Combating Multilateral Development Bank Corruption: U.S. Treasury Role and Internal Efforts*. As expressed by the Committee Chair (Senator Lugar), concerns were raised that the Department was "unable to dedicate sufficient resources to investigate the use of those funds."

Preceding that hearing, the Committee had forwarded correspondence to our office requesting we look into allegations of a multi-million dollar "embezzlement of public funds"

involving the World Bank. Absent any apparent means by which to bring about criminal, civil or administrative fraud-related remedies (i.e., no documentation and/or certification submissions being required by the World Bank, MDBs, or other entities interacting with Treasury-led funding activities), Treasury OIG met with the Committee to work through procedural, jurisdictional, and potential statutory authority issues. We also advised the Committee that the embezzlement allegation was referred to other OIG investigative programs that might have more direct oversight of the MDBs (the U.S. Department of State and the U.S. Agency for International Development).

In keeping with our commitments made to Committee staff, Treasury OIG continues liaison with OIA and the World Bank to develop additional information.

Integrity Awareness Briefings

Integrity awareness remains a high priority for the Treasury OIG as it is critical to the effectiveness of agency programs in that it affects how the programs are perceived throughout the federal government and received by the citizens they serve.

We conducted two fraud and integrity awareness briefings with BEP employees, managers and supervisors during the reporting period. The OIG is working with all the Treasury components to ensure they have programs in place to brief each employee on fraud and integrity awareness as well as ethical conduct.

In FY 2005, the OIG will be working with ethics officials throughout DO and the Treasury bureaus and will be conducting additional Integrity Awareness briefings with them, including the BEP's facility in Fort Worth, Texas.

Summary of OIG Activity

For the Year Ended September 30, 2004

OIG Activity	10/1/2003 – 3/31/2004	4/1/2004 – 9/30/2004	Fiscal Year Total
General			
Regulation and Legislation Reviews	85	65	150
Instances Where Information was Refused	1 instance – see discussions on pages 28 and 36		
Office of Audit Activities			
Reports Issued (Audits and Evaluations)	31	18	49
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	$0	$0
b) Funds Put to Better Use	$0	$0	$0
c) Revenue Enhancements	$0	$0	$0
Total Monetary Benefits	$0	$0	$0
Office of Investigations Activities			
Reports of Investigation	7	5	12
Preliminary Inquiry Closing Memorandums	8	4	12
Number of OIG Hotline Calls Processed	922	1,239	2,161
Allegations – Total Number Processed	238	211	449
Referrals Made During the Period	165	101	266
Cases Open at Start of Period	47	54	47 Start
Cases Opened in the Reporting Period	30	58	88
Cases Closed in the Reporting Period	23	6	29
Cases Open at the End of the Period	54	106	106 End
Inquires Open at Start of Period	5	10	5 Start

OIG Activity	10/1/2003 – 3/31/2004	4/1/2004 – 9/30/2004	Fiscal Year Total
Inquiries Opened in the Reporting Period	14	23	37
Inquiries Closed in the Reporting Period	9	5	14
Inquiries Open at the End of the Period	10	28	28 End
Judicial Actions			
Cases Referred for Prosecution	9	28	37
Cases Accepted for Prosecution	3	26	29
Arrests	8	36	44
Search Warrants	3	13	16
Indictments/Information	15	17	32
Pleas	3	4	7
Conviction by Trial	0	2	2
Imprisonment (Months)	6	27	33
Home Detention (Months)	0	12	12
Probation (Months)	24	108	132
Community Service (Hours)	0	25	25
Administrative Sanctions			
Adverse Personnel Actions	1	5	6
Contractor Suspensions/Debarments	3	1	4
Individual Suspensions/Debarments	0	4	4
Oversight Activities			
Quality Assessment Reviews	1	1	2
Management Implication Reports	0	2	2
Fraud and Integrity Briefings	0	2	2
Monetary Benefits			
Fines	$0	$2,500	$2,500
Restitution	$0	$0	$0
Recoveries	$153,000	$0	$153,000
Settlements	$0	$350,000	$350,000
Savings/Cost Avoidance	$0	$643,500	$643,500
Actual Losses Identified	$63,292,600	$161,888,570	$225,181,170
Potential Losses Identified	$470,422	$2,491,018	$2,961,440

Significant Unimplemented Recommendations

For Reports Issued Prior to September 30, 2003

Report Number	Issue Date	Report Title and Recommendation Summary
OIG-01-014	11/00	*Review of Treasury Computer Security Plans* The Treasury CIO should: (i) correct system vulnerabilities identified in DO systems, update DO system security plans, ensure through the certification and accreditation process that system security plans are kept up-to-date and that new system vulnerabilities are identified and addressed; and (ii) develop a means to identify all existing and newly developed DO systems. (1 recommendation)
OIG-02-115	9/02	*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) develops a strategy to consolidate and minimize the number of smart card and PKI administrative systems (inventory management, personnel management, administrative, travel, manpower, etc.); (5) uses another hard token as an interim security measure along with smart cards to provide strong two-factor authentication for digital certificates; and (6) establishes appropriate record management controls for general, sensitive, and secret information related to the Treasury smart card and PKI infrastructure. (6 recommendations)
OIG-02-122	9/02	*Community Development Financial Institution (CDFI) Fund* The CDFI Fund Director should initiate action to amend the OMB Circular A-133 Compliance Supplement to reflect revised accountability requirements for financial assistance funds. (1 recommendation)
OIG-03-004	10/02	*The Bureau of Engraving and Printing's Controls Over Background Investigations Need to be Improved* The Bureau should designate someone to provide continuous oversight over both facilities (Washington, DC and Ft. Worth) relative to background investigations and other applicable security issues. A self-assessment of the Ft. Worth facility should be performed. (1 recommendation)
OIG-03-007	10/02	*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)
OIG034	12/02	*Audited Financial Statements of the Treasury Forfeiture Fund for Fiscal Years 2002 and 2001* EOAF should for all direct costs and common support costs not directly traceable to individual seizures: (1) develop and implement an allocation process. Indirect costs will have to be applied to the individual seizures. Direct and indirect costs will have to be added together to provide total costs seizure; and (2) vigorously pursue the enhancement of SEACATS system capabilities to record and report expenses at the asset level. (2 recommendations)

Significant Unimplemented Recommendations

For Reports Issued Prior to September 30, 2003

Report Number	Issue Date	Report Title and Recommendation Summary
OIG-03-035	12/02	*Financial Crimes Enforcement Network: Reliability of Suspicious Activity Reports* OIG Note: According to Treasury's automated audit recommendation tracking system, FinCEN completed all planned corrective actions by September 30, 2004. The OIG has a follow-up audit in progress.
OIG-03-038	12/02	*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-03-093	8/03	*INFORMATION TECHNOLOGY: Treasury's Cyber-Based Critical Infrastructure Protection Implementation Efforts Remain Inadequate* The Treasury CIO should finalize draft documents that are key elements of the Treasury Critical Infrastructure Protection Plan and distribute them to DO and the bureaus, ensuring that DO and the bureaus have the necessary guidance to comply with PDD 63 requirements. (1 recommendation)

This list of unimplemented recommendations in OIG audit reports 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, 2004, through September 30, 2004

The OIG sought information from OCC in connection with an investigation involving a failed bank. OCC questioned the OIG's jurisdiction, and refused to provide information. We brought this matter to the Secretary's attention, pursuant to IG Act § 6(b) (2), as well as to the House and Senate oversight committees. The OIG is continuing efforts to resolve the dispute.

Listing of Audit and Evaluation Reports Issued

April 1, 2004, through September 30, 2004

Financial Audits and Attestation Engagements

DO, FINANCIAL MANAGEMENT: Department of the Treasury Payments for Water and Sewer Services Provided by the District of Columbia Were Made Timely for the Third Quarter of Fiscal Year 2004; OIG-04-030, 4/15/2004

FMS, Audit of the Financial Management Service's Fiscal Years 2003 and 2002 Schedules of Non-Entity Government-Wide Cash; OIG-04-031, 4/23/04

Listing of Audit and Evaluation Reports Issued

April 1, 2004, through September 30, 2004

FMS, Management Letter for Fiscal Year 2003 Audit of the Financial Management Service's Schedules of Non-Entity Government-Wide Cash; OIG-04-032, 5/4/04 (LOU)

MINT, Audit of the United States Mint's Fiscal Years 2003 and 2002 Financial Statements; OIG-04-033, 5/18/04

DO, Treasury Payment for DC Water and Sewer Services for Fourth Quarter of FY 2004; OIG-04-036, 7/15/04

FMS, Audit of the Financial Management Service's Fiscal Years 2003 and 2002 Schedules of Non-Entity Assets, Non-Entity Costs and Custodial Revenue; OIG-04-037, 7/19/04

FMS, Management Letter for Fiscal Year 2003 Audit of the Financial Management Service's Schedule of Non-Entity Assets, Non-Entity Costs and Custodial Revenue; OIG-04-038, 7/19/04 (LOU)

BPD, Controls Placed in Operation and Tests of Operating Effectiveness for the Treasury Bureau of the Public Debt Administrative Resource Center Accounting Services Division for the Period July 1, 2003 to June 30, 2004; OIG-04-040, 9/2/04

BPD, Controls Placed in Operation and Tests of Operating Effectiveness for the Treasury Bureau of the Public Debt Trust Fund Management Branch for the Period October 1, 2003 to July 31,2004; OIG-04-041, 9/14/04

BPD, Controls Placed in Operation and Tests of Operating Effectiveness for the Treasury Bureau of the Public Debt Federal Investments Branch for the Period of October 1, 2003, to July 31, 2004; OIG-04-042, 9/14/04

Information Technology Evaluations

DO, Intelligence Sharing; OIG-CA-04-003, 4/14/2004 (Classified)

DO, INFORMATION TECHNOLOGY: Fiscal Year 2004 Evaluation of Treasury's FISMA Implementation for Its Intelligence Program; OIG-CA-04-006, 8/15/04 (Classified)

Listing of Audit and Evaluation Reports Issued

April 1, 2004, through September 30, 2004

Performance Audits and Evaluations

OCC and OTS, SAFTETY, SOUNDNESS, AND ACCESSIBILITY OF FINANCIAL SERVICES: Summary of Treasury OIG's Material Loss Reviews of Failed National Banks and Thrift Institutions Between 1993 and 2002; OIG-CA-04-004, 5/28/2004

DO, GENERAL MANAGEMENT: Summary Report on Weaknesses in Treasury Bureau Purchase Card Program; OIG-04-034, 6/18/04

BEP, GENERAL MANAGEMENT: Control Over Security Need to be Improved at the Bureau of Engraving and Printing; OIG-04-035, 6/26/04 (LOU)

DO, GENERAL MANAGEMENT: Treasury's Rural Development Act Policy; OIG-CA-04-005, 7/16/2004

DO, GENERAL MANAGEMENT: Management of the Treasury Building and Annex Repair and Restoration Program Needs to Be Strengthened; OIG-04-039 (Interim Report), 8/9/04

DO, GENERAL MANAGEMENT: Treasury Building and Annex Repair and Restoration Program Procurement Practices Need to be Improved; OIG-04-043 (Interim Report), 9/23/04

Number of Audit and Evaluation Reports by Bureau

April 1, 2004 through September 30, 2004

Office/Bureau	Number of Reports
BEP	1
BPD	3
Departmental Offices	8
FMS	4
Mint	1
OCC and OTS	1
Total	18

Audit Reports Issued with Questioned Costs

April 1, 2004, to September 30, 2004 (Dollars in Thousands)

Category	Total		
	No. of Reports	Questioned Costs	Unsupported Costs
For which no management decision had been made by beginning of reporting period	3	$1,151	0
Which were issued during the reporting period	0	$0	0
Subtotals	3	$1,151	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	3	$1,151	0
For which no management decision was made within 6 months of issuance	3	$1,151	0

"Questioned costs" 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. During the period, there were no reports with unsupported costs.

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

April 1, 2004, to September 30, 2004 (Dollars in Thousands)

Category	No. of Reports	Total	Savings	Revenue Enhancement
For which no management decision had been made by the beginning of the reporting period	0	0	0	0
Which were issued during the reporting period	0	0	0	0
Subtotals	0	0	0	0
For which a management decision was made during the reporting period	0	0	0	0
Dollar value of recommendations agreed to by management	0	0	0	0
based on proposed management action	0	0	0	0
based on proposed legislative action	0	0	0	0
dollar value of recommendations not agreed to by management	0	0	0	0
For which no management decision has been made by the end of the reporting period	0	0	0	0
For which no management decision was made within 6 months of issuance	0	0	0	0

A recommendation that funds be put to better use denotes funds could be used more efficiently if management took actions to implement and complete the recommendation including: (1) reduction in outlays, (2) de-obligations of funds from programs or operations, (3) costs not incurred by implementing recommending improvements related to operations, (4) avoidance of unnecessary expenditures noted in pre-award review of contract agreements, (5) any other savings which are specifically identified, or (6) enhancements to revenues.

Previously Issued Audit Reports Pending Management Decisions

As of September 30, 2004 (Dollars in Thousands)

Title and Date Issued	Report Number	Amount	Bureau
Costs Incurred Under Contract TOS-91-31 for Calendar Year 1991, 3/12/96 a/	OIG-96-042	$5	DO
Contractor's FY Ended December 31, 1992 through 1994, Applicable to Contracts TOS-91-31 and TOS-94-25, 2/25/98 a/	OIG-98-045	$562	DO
Incurred Cost for Contract TOS-92-20 for FY 1997, 1/7/00 b/	OIG-00-030	$584	DO
Totals	**3 Reports**	**$ 1,151**	

a/ Contract negotiations are currently on-going.
b/ Contract modification issued to close contract.

Significant Revised Management Decisions

April 1, 2004 to September 30, 2004

There were no significant revised management decisions during the period.

Significant Disagreed Management Decisions

April 1, 2004 to September 30, 2004

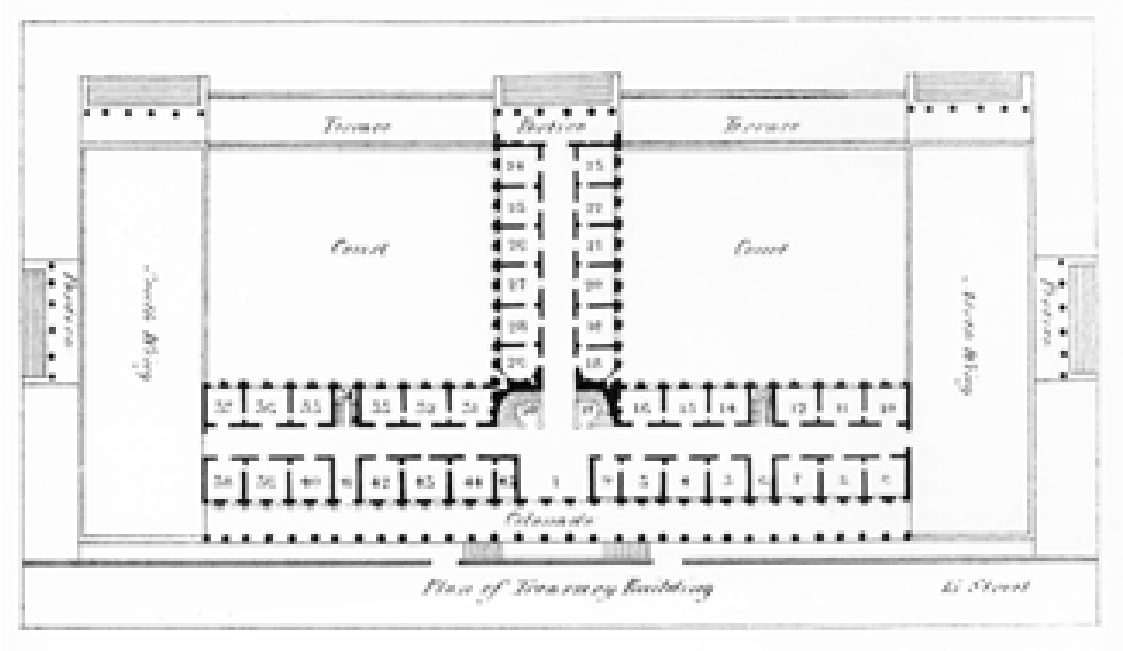
There were no management decisions this period with which the Inspector General was in disagreement.

Reference to the Inspector General Act of 1978, as Amended

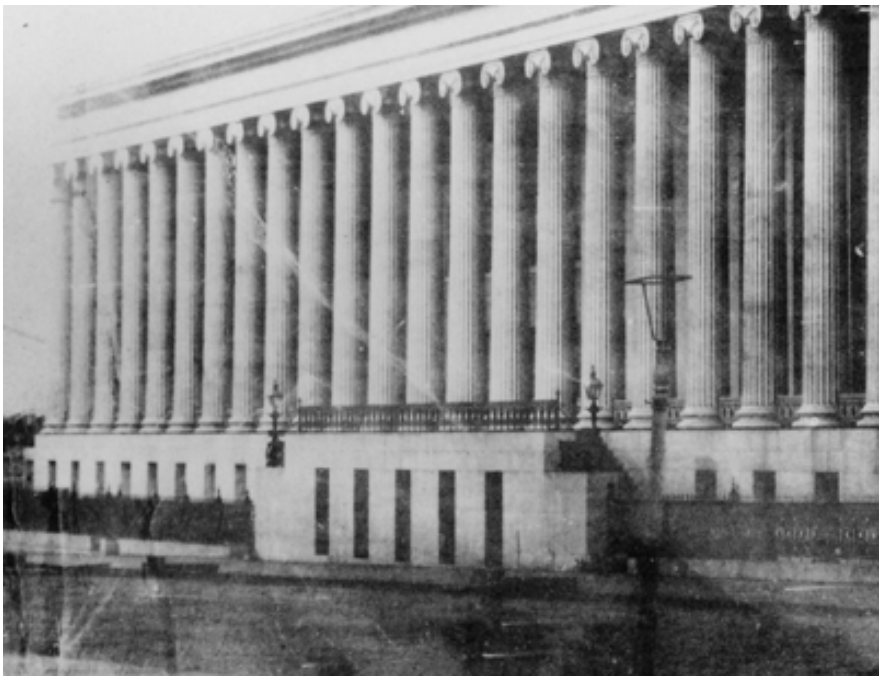
Reference	Requirement	Page
Section 4(a)(2)	Review of legislation and regulations	35
Section 5(a)(1)	Significant problems, abuses, and deficiencies	5-24
Section 5(a)(2)	Recommendations with respect to significant problems, abuses, and deficiencies	5-24
Section 5(a)(3)	Significant unimplemented recommendations described in previous semi-annual reports	35
Section 5(a)(4)	Matters referred to prosecutive authorities	34
Section 5(a)(5)	Summary of instances where information was refused	36
Section 5(a)(6)	List of audit reports	36
Section 5(a)(7)	Summary of significant reports	39
Section 5(a)(8)	Audit Reports with questioned costs	38
Section 5(a)(9)	Recommendations that funds be put to better use	40
Section 5(a)(10)	Summary of audit reports issued before the beginning of the reporting period for which no management decision has been made	40
Section 5(a)(11)	Significant revised management decisions made during the reporting period	41
Section 5(a)(12)	Management decisions with which the Inspector General is in disagreement	41
Section 5(a)(13)	Instances of unresolved FFMIA non-compliance	5
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	28

ABA	Architectural Barriers Act
ARC-ASD	Administrative Resource Center Accounting Services Division, BPD
ATSB	Air Transportation Stabilization Board
BEP	Bureau of Engraving and Printing
BOE	Bill of Exchange
BPD	Bureau of the Public Debt
BSA	Bank Secrecy Act
CDFI Fund	Community Development Financial Institutions Fund
CFO	Chief Financial Officer
COTR	Contracting Officers' Technical Representative
CIO	Chief Information Officer
DC	District of Columbia
DCAA	Defense Contract Audit Agency
DO	Departmental Offices
EDS	Employee Development Specialist
ESF	Exchange Stabilization Fund
FBI	Federal Bureau of Investigation
FDIC	Federal Deposit Insurance Corporation
FFB	Federal Financing Bank
FFMIA	Federal Financial Management Improvement Act of 1996
FIB	Federal Investments Branch, BPD
FinCEN	Financial Crimes Enforcement Network
FISMA	Federal Information Security Management Act
FMS	Financial Management Service
FTE	Full-time Equivalent
FY	Fiscal Year
H.R.	House Report
IPA	Independent Public Accountant
IRS	Internal Revenue Service
Keystone	First National Bank of Keystone
LOU	Limited Official Use
MAFTF	Metro Area Fraud Task Force
Mint	U.S. Mint
MIR	Management Implication Report
OA	Office of Audit
OC	Office of Counsel
OCC	Office of the Comptroller of the Currency
OCS	Operation Card Shark
ODCP	Office of D.C. Pensions
OFAC	Office of Foreign Assets Control
OI	Office of Investigations
OIG	Office of Inspector General
OMB	Office of Management and Budget
OTA	Office of Technical Assistance

OTS	Office of Thrift Supervision
PKI	Public Key Infrastructure
RTA	Resident Tax Advisor
SAR	Suspicious Activity Report
SEACATS	Seized Assets and Case Tracking System
Secret Service	U.S. Secret Service
SNB	Sinclair National Bank
TBARR	Treasury Building and Annex Repair and Restoration
TD	Treasury Directive
TEOAF	Treasury Executive Office for Asset Forfeiture
TFF	Treasury Forfeiture Fund
TFI	Office of Terrorism and Financial Intelligence
TFMB	Trust Fund Management Division, BPD
TIGTA	Treasury Inspector General for Tax Administration
Treasury	Department of the Treasury
TTB	Alcohol and Tobacco Tax and Trade Bureau
USAO–DC	U.S. Attorney's Office for the District of Columbia
USC	United States Code
UQ	Unqualified Opinion
WCF	Western Currency Facility, BEP



The Treasury Building, constructed between 1836 and 1869, is one of the country's finest examples of Greek Revival architecture. It served as the temporary White House for President Andrew Johnson and its splendid Cash Room was the site of President Ulysses S. Grant's Inaugural Reception. *(Source: The Treasury Historical Society)* Above is architect Robert Mill's floor plan for the building, and below is an 1856 photograph of the east façade. As discussed on page 9, the Building is currently undergoing a major renovation project. As part of the Consolidated Appropriations Act, 2004, the Congress directed our office to audit this effort. During this Semiannual period, we issued two Interim Audit Reports on our ongoing audit.



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) 927-5799

Office of Counsel
740 15th Street, N.W., Suite 510
Washington, D.C. 20220
Phone: (202) 927-0650; Fax: (202) 927-6492

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
Boston, Massachusetts 02110-3350
Regional Inspector General for Audit, Room 330
Phone: (617) 223-8640; Fax: (617) 223-8651

Western Field Audit Office
333 Market Street
San Francisco, California 94105
Regional Inspector General for Audit, Suite 275
Phone: (415) 977-8810; Fax: (415) 977-8811

Treasury OIG Hotline
Call Toll Free: 1.800.359.3898

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