Semiannual Report To The Congress

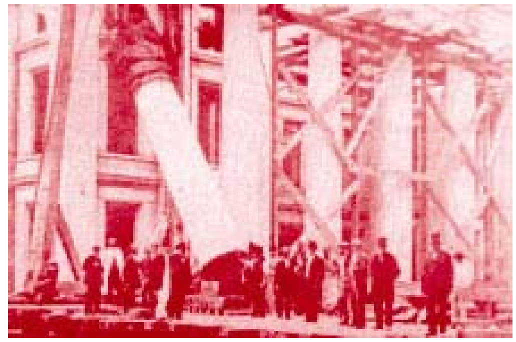
October 1, 2002 –March 31, 2003

Office of Inspector General

DEPARTMENT OF THE TREASURY

About Treasury

Congress enacted a law on September 2, 1789, which created the Department of the Treasury, thereby making it the second oldest department in the Federal government. Starting with our first Secretary, Alexander Hamilton (1789-1795), through our current Secretary, John Snow (2003 – present), 73 individuals have committed time in their lives to the responsibility of managing our country's finances. Over time the role of Treasury has expanded greatly. Present duties and functions include:



- $$ Collecting taxes, duties, and monies paid to and due to the U.S. and paying all bills of the U.S.
- $$ Producing currency, coinage, and postage stamps
- $$ Managing Government accounts and the public debt
- $$ Supervising national banks and thrift institutions
- $$ Advising on domestic and international financial, monetary, economic, and trade policy
- $$ Combating money laundering, including terrorist financing, and other financial crimes
- $$ Investigating and prosecuting tax evaders, counterfeiters, forgers, smuggle spirits distillers, and gun law violators
- $$ Protecting the President, Vice President, their families, candidates for those offices, foreign missions resident in Washington and visiting foreign dignitaries

April 30, 2003

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

Dear Mr. Secretary:

Enclosed is my Semiannual Report to the Congress. This report summarizes the activities of the Office of Inspector General (OIG) for the 6-month period ending March 31, 2003, and highlights both the important accomplishments and some serious deficiencies in the Department's programs and operations.

During this semiannual period, the OIG has seen a profound change in its size and capability with the divestiture of most of our personnel and resources to the Department of Homeland Security. We no longer have the resources necessary to provide timely audit and investigations services to the Department.

Sincerely,

Jeffrey Rush, Jr.
Inspector General

Enclosure

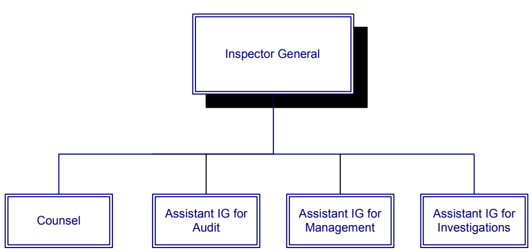
Table of Contents

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 § 1. 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's program and operations and keeps the Secretary of the Treasury and Congress fully informed of problems, deficiencies, and the need for corrective action.

During FY 2003, the OIG had a budget of $35.7 million and a staff of 282 full-time civil servants. On March 1, 2003, a significant portion of the OIG's workforce and resources transferred to the new Department of Homeland Security (DHS) pursuant to the Homeland Security Act of 2002.

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



The Office of Audit (OA) performs program, financial, information technology, and contract audits. The Assistant Inspector

General for Audit (AIGA) has two deputies. One deputy is assigned to program audits while the other deputy is assigned to financial management and information technology audits. OA headquarters is located in Washington, DC, and it maintains a regional office in San Francisco. Pre-divestiture of staff and resources to DHS OIG, OA also maintained field offices located in Boston, Chicago, and Houston and suboffices in Marlton, NJ, Indianapolis, Miami, and Los Angeles.

The Office of Investigations (OI) performs investigations aimed at the detection and prevention of fraud, waste, and abuse in Treasury programs and operations. During this period OI also provides direct oversight of the internal investigations performed by the Offices of Inspection of the Bureau of Alcohol, Tobacco and Firearms (ATF) and the United States Secret Service (Secret Service), and the Office of Internal Affairs of the United States Customs Service (Customs) before these agencies transferred to Justice and DHS pursuant to the Homeland Security Act. The Assistant Inspector General for Investigations (AIGI) has a deputy who is responsible for day-to-day operations. The immediate office of the AIGI develops OI policy and procedures in addition to administrating OI's budget and records management. OI headquarters also maintains the Hotline and conducts sensitive inquiries of high-level Treasury officials. OI headquarters is located in Washington, DC, and is supported by a field office in the metropolitan area. Pre-divestiture, OI also maintained five regional offices located in Chicago, Houston, Philadelphia, Miami, San Francisco, and one sub-office in Los Angeles.

Office of Management (OM) 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, office policy preparation, planning, and reporting for the OIG. The Assistant Inspector General for Management is in charge of these functions.

Our Office

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 OI and OA. The OC 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. Finally, the OC conducts the OIG's ethics training, financial disclosure, and Freedom of Information Act programs.

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 fairness, 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.

Regarding Our Divestiture

The Homeland Security Act of 2002, P.L. 107-296 (HSA), became law in November 2002. It created the Department of Homeland Security (DHS), into which transferred Customs, Secret Service, and the Federal Law Enforcement Training Center (FLETC) from Treasury. The HSA established an Inspector General in the new Department. During Congress' consideration of this legislation, the Treasury OIG recommended that the bill continue the system of oversight of the internal investigative programs relating to those law enforcement bureaus that existed when they were in the Treasury. This requirement was included in the HSA.

In addition to the transfers of Customs, Secret Service and FLETC, the HSA transferred the law enforcement activities of ATF to the Department of Justice, where they are included in the newly created Bureau of Alcohol, Tobacco, Firearms and Explosives. The HSA kept the revenue functions of the former ATF within the Treasury as part of the newly-established Alcohol and Tobacco Tax and Trade Bureau (TTB). Under the amended legislation, the TTB has internal investigative capabilities, with Treasury OIG oversight.

Section 1516 of the HSA authorizes the Director of the Office of Management and Budget (OMB) to direct further transfers of personnel, assets, and programs to carry out the purposes of the HSA. Pursuant to this authority, OMB proposed a plan to have the Treasury OIG transfer personnel and budget authority to both the Departments of Justice and Homeland Security OIGs. The Department of Justice OIG was also required to transfer personnel and budget authority to the DHS OIG. The three affected Inspectors General agreed, with the concurrence of OMB, to net the effect of these required transfers. Thus all of Treasury OIG transfers went to the DHS OIG-- none of these transfers went to the Justice OIG. This agreement reduced the number of transfers from the Department of Justice OIG to the DHS OIG.

About Treasury

Treasury's mission is to (1) promote prosperous and stable American and world economies, (2) manage the Government's finances, (3) safeguard our financial systems, (4) protect our Nation's leaders, (5) secure a safe and drug-free America, and (6) continue to build a strong institution. Organized into offices and bureaus, the Treasury encompasses a wide range of programmatic and operational activities. Prior to the divestiture, more than 160,000 people made up the Treasury.

Alcohol and Tobacco Trade and Tax 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 Alcohol, Tobacco and Firearms (ATF) oversees and enforces laws relating to the use of firearms, explosives, alcohol, and tobacco.[1]

Bureau of Engraving and Printing (BEP) manufactures paper currency and postage stamps.

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

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

U.S. Customs Service (Customs) protects the Nation's borders, facilitates international trade, and collects duties and other forms of revenue.[2]

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

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

Federal Law Enforcement Training Center (FLETC) provides government-wide law enforcement training.

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 Inspector General (OIG) provides independent and objective reviews of Treasury operations.

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

U.S. Secret Service (Secret Service) protects National leaders and foreign dignitaries and enforces counterfeiting and financial crime laws.

Treasury Inspector General for Tax Administration (TIGTA) provides independent and objective reviews of IRS activities.

[1] The law enforcement functions of ATF were divested to Justice under HSA. The revenue functions are retained in the Department as part of the TTB

[2] Customs, FLETC, and Secret Service were divested to DHS by the HSA

Improving Treasury's Internal Operations

Financial And Financial Related Audits

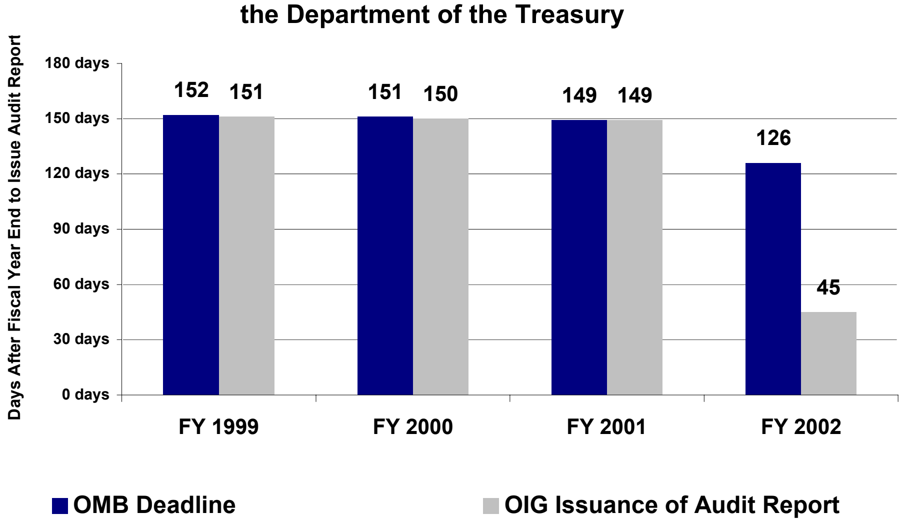
Consolidated Financial Statements

The OIG issued unqualified opinions on the Treasury's financial statements for FYs 2002 and 2001. There were four material weaknesses in internal control related to (1) financial management and reporting at the IRS; (2) electronic data processing controls, most notably at IRS, Customs, FMS, and the Mint; (3) management of trade activities and related systems at Customs; and (4) FMS' controls over outstanding checks. Also, Treasury's financial systems were not in substantial compliance with Federal Financial Management Improvement Act (FFMIA) requirements.

FY 2002 represented a breakthrough year in terms of accelerating the completion of annual financial statement audits and enabling the Department to issue its FY 2002 Performance and Accountability Report by November 15, 2002. This is more than 3 months ahead of last year's schedule, and 2 years in advance of the OMB's requirement that FY 2004 reports be submitted by November 15th.

While this is a truly remarkable accomplishment, costly and labor-intensive procedures were still necessary to produce reliable financial statements, albeit within a shorter time frame. Only limited progress has been made in addressing major longstanding financial management and systems deficiencies that persist at key bureaus. Also, new material weaknesses were identified at Customs and FMS.
The Department has taken steps to address material weaknesses and other deficiencies; however, these efforts need to be intensified and broadened. In addition to focusing on correcting conditions identified in prior years, the Department should take a proactive approach and assess controls throughout the year. One of management's goals should be to discover and correct internal control problems before the auditors report them. We will continue to audit and opine on the Department's consolidated financial statements. However, effective March 1, 2003, DHS assumed responsibility for addressing Customs' internal control material weaknesses. In addition, Justice will be responsible for resolving reportable conditions relating to the former ATF. (OIG-03-014)

Accelerated Audited Financial Statements for the Department of the Treasury



Improving Treasury's Internal Operations

Treasury's financial systems continue to not substantially comply with the requirements of the FFMIA. The following table reflects instances of non-compliance reported in connection with our FY 2002 financial statement audits. In addition, we reviewed the Department's oversight of corrective actions in order to address FFMIA non-compliances identified in the prior years' financial statement audits, to include whether remediation plans were developed and whether major milestones were achieved. Treasury is making progress in achieving compliance. However, in certain cases, notably Customs, key milestone dates have been extended. Specifically, Customs has extended the scheduled completion date from October 2003 to October 2004 for certain corrective actions needed to address the longstanding material weakness related to the core financial system. The reason for this extension is due to insufficient funding to support subsidiary ledger development. This highlights the need to clearly link corrective action plans with spending plans in order to anticipate difficulties in meeting scheduled milestones.

We recommended that the Department strengthen its oversight of the remediation process in three areas: (1) ensure that current FFMIA guidance is updated, as needed, to provide additional detailed information required for the submission of remediation plans, (2) continue to develop the expertise necessary to allow for a more detailed assessment of remediation plans, and (3) seek opportunities to ensure that conditions that allowed for existing material weaknesses are remedied throughout Treasury, thus helping to reduce or eliminate future occurrences. As a result of the divestiture under the HSA, DHS or Justice management is responsible for determining whether financial systems of transferred Treasury activities and bureaus comply with FFMIA requirements. (OIG-03-025)

Improving Treasury's Internal Operations

Entity	Condition	FY First Reported for FFMIA Purposes	Type of Non-Compliance
Customs	Core financial systems do not provide complete and accurate information for financial reporting and for preparation of audited financial statements.	1997	Federal Financial Management Systems Requirements (FFMSR), Standard General Ledger (SGL)
FMS	General control weaknesses may affect information in FMS system.	1997	FFMSR
IRS	The general ledger does not conform to the U.S. Government Standard General Ledger.	1997	SGL
IRS	The bureau lacks a reliable subsidiary ledger for its property and equipment.	1997	FFMSR
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 included controls over the financial reporting process, unpaid tax assessments, tax revenue and refunds, property and equipment, and computer controls.	1997	FFMSR, Federal Accounting Standards
IRS	IRS cannot rely on information from its general ledger to prepare financial statements.	1997	FFMSR
IRS	IRS lacks a subsidiary ledger for unpaid assessments.	1997	FFMSR
Mint	Weaknesses exist in the Mint information system general controls.	2001	FFMSR
Customs	IT system logical access and software maintenance security controls need improvement	2002	FFMSR
Customs	Material weaknesses related to controls over the entry process and drawback claims.	2002	Federal Accounting Standards
FMS	Material weakness related to controls over outstanding checks.	2002	Federal Accounting Standards

Other Financial Audits

The Chief Financial Officers (CFO) Act, as amended by the Government Management Reform Act (GMRA), requires annual audits of Treasury and OMB designated components. OMB has designated ATF, Customs, and IRS for annual financial statement audits. However, ATF and Customs received a waiver from this requirement for FYs 2001 and 2002. Certain other components are audited pursuant to other requirements, or due to their materiality to Treasury. The following table shows audit results for FYs 2002 and 2001.

Improving Treasury's Internal Operations

Treasury Audited Financial Statements And Related Audits

Entity	FY2002 Audit Results: Opinion	FY2002 Audit Results: Material Weaknesses	FY2002 Audit Results: Other Reportable Conditions	FY2001 Audit Results: Opinion	FY2001 Audit Results: Material Weaknesses	FY2001 Audit Results: Other Reportable Conditions
GMRA/CFO Requirements						
Treasury Department	UQ	4	0	UQ	2	2
ATF	(A)	-	2	(A)	-	-
Customs	(A)	4	5	(A)	-	-
IRS (B)	UQ	5	2	UQ	6	1
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
Exchange Stabilization Fund	UQ	0	0	UQ	0	2
Federal Financing Bank	UQ	0	0	UQ	0	0
OCC	UQ	0	1	UQ	0	2
OTS	UQ	0	0	UQ	0	0
Treasury Forfeiture Fund	UQ	0	1	UQ	0	2
Mint						
Financial Statements	(C)	(C)	(C)	UQ	2	1
Custodial Gold and Silver Reserves	UQ	0	0	UQ	0	0
Material to Treasury Department Financial Statements						
BPD						
Schedule of Federal Debt (B)	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 Federal Government	UQ	2	0	UQ	1	0

UQ =Unqualified opinion rendered.
(A) The Department requested and received waivers from OMB for the requirement for stand-alone audited financial statements for ATF and Customs for FYs 2001 and 2002. For FY 2001, limited audit work was performed at these two entities to support the audit of the Department's financial statements. For FY 2002, an examination of internal control over financial reporting at Customs resulted in a qualified opinion, and identified 4 material weaknesses and 5 reportable conditions. A similar examination at ATF identified reportable conditions related to information technology general and application control weaknesses.
(B) Audited by the U.S. General Accounting Office.
(C) Audit report was not issued as of March 31, 2003.

The results of financial audits and internal control examinations performed in support of our audit of the Department's FY 2002 consolidated financial statements or required by statute are summarized as follows:

Improving Treasury's Internal Operations

- An independent public accountant (IPA) rendered an unqualified opinion on the **FMS**' FYs 2002 and 2001 Schedules of Non-Entity Government-wide Cash. The auditors reported two material weaknesses. The first material weakness related to the effectiveness of computer controls. In this regard, there were numerous general control weaknesses at the Hyattsville Regional Operations Center that did not effectively prevent (1) unauthorized access to and disclosure of sensitive information, (2) unauthorized changes to systems and application software, (3) unauthorized access to certain programs and files, or (4) disruption of critical operations. There were also weaknesses in certain application controls.

  The second material weakness related to the following problems associated with controls over outstanding checks: (1) until recently, FMS was unable to produce a detail of outstanding checks as of a given date, (2) FMS did not reconcile the balance of outstanding checks in the general ledger to the subsidiary system, (3) certain reconciling items affecting the general ledger were not investigated and related adjustments were not made in the proper period, and (4) reconciliation procedures between certain systems that track check-status related data were insufficient. Due to the lack of reconciliation controls and the lack of an adequate audit trail for outstanding checks, a misstatement of government-wide cash went undetected. FMS was unable to determine the cause of a $3.1 billion overstatement of cash, the cause of the related understatement of outstanding checks, or when the misstatement occurred. FMS determined that the understatement of outstanding checks occurred prior to September 30, 2000. FMS corrected the misstatement.

  With respect to laws and regulations, FMS was not in compliance with OMB Circulars A-127 "Financial Management Systems" and A-130 "Management of Federal Information Resources." These Circulars require a comprehensive security plan, controls to protect information, and a fully developed and tested contingency plan. (OIG-03-039)

- An IPA's examination of **Customs'** internal control over financial reporting as of and for the fiscal year ended September 30, 2002, resulted in a qualified opinion due to scope limitations and four material weaknesses. With respect to the scope limitations, security clearance procedures and other matters related to access and handling sensitive information delayed the start of the information technology evaluation. The delay prevented the IPA from completing test work on information technology general and application controls.

  The IPA identified four material weaknesses: (1) Customs did not adequately monitor the effectiveness of its internal controls over entry duties and taxes in FY 2002; (2) drawback controls needed to be strengthened; (3) information technology system logical access and software maintenance security controls needed to be improved; and (4) core financial systems needed to be improved and integrated. The IPA also identified five reportable conditions.

  The FY 2002 audit results at Customs indicate deterioration since FY 2000 in financial management and internal controls. The last full scope financial statement audit at Customs was performed in FY 2000. Two material weaknesses were identified in the FY 2000 audit, including improvements needed in core financial systems, which was first reported in FY 1992. The continuing deficiencies in Customs financial management pose significant risks because Customs has been incorporated into the newly established DHS. Management should assign a high priority and make a firm commitment to finally resolving these chronic weaknesses. Audit follow-up is the responsibility of DHS. (OIG-03-033 and OIG-03-064)

- An IPA concluded that **ATF** maintained, in all material respects, effective internal control over financial reporting as of and for the fiscal year ended September 30, 2002. The IPA noted two reportable conditions related to information technology general and application controls and other matters involving internal control over financial reporting. Audit follow-up for ATF law enforcement activities is the responsibility of Justice. (OIG-03-044 and OIG-03-052)

- The **Treasury Forfeiture Fund** (TFF) received an unqualified opinion on its financial statements for FYs 2002 and 2001. However, as noted in the last audit report, total asset specific expenses were not recorded and accounted for by the TFF. Although holding costs and direct selling costs related to real property and vehicles were captured in the Seized Assets and Case Tracking System, indirect overhead expenses of the national seized property contractor were not recorded and accounted for by the TFF at the line item level. This condition can impact equitable sharing expenses of the TFF. No instances of reportable noncompliance with laws and regulations were found. (OIG-03-034)

- An IPA issued an unqualified opinion on **OCC**'s FYs 2002 and 2001 financial statements. The IPA noted, as a reportable condition, that $MART (Management and Accountability Reporting Tools) system controls needed to be strengthened. OCC implemented $MART, an integrated financial and acquisitions management system, in October 2001. The IPA identified deficiencies in application security controls, infrastructure security, and Information Technology (IT) operational controls. Specifically, procedures for the administration of $MART user accounts did not exist, risk assessments for general support systems and major applications were not complete, and the $MART security plan contained inaccurate control descriptions. In addition, documentation supporting requests, program changes, testing and acceptance for the $MART system needed to be improved, and disaster recovery capabilities tested. (OIG-03-016)

- Our office or IPAs under our oversight issued unqualified opinions and noted no reportable conditions in internal control or reportable instances of non-compliance with laws and regulations for the financial statements or schedules prepared by the following bureaus and funds: (1) **OTS**' FY 2002 financial statements (OIG-03-017); (2) **BEP**'s FY 2002 financial statements (OIG-03-046); (3) **Departmental Offices**' FYs 2002 and 2001 financial statements (OIG-03-020); (4) **Office of DC Pensions**' FYs 2002 and 2001 financial statements (OIG-03-018); (5) **Exchange Stabilization Fund**'s FYs 2002 and 2001 financial statements (OIG-03-037); (6) **Community Development Financial Institutions Fund**'s FYs 2002 and 2001 financial statements (OIG-03-048); (7) **Federal Financing Bank**'s FYs 2002 and 2001 financial statements (OIG-03-028); (8) **Mint**'s FYs 2002 and 2001 Schedule of Custodial Gold and Silver Reserves; (9) Schedule of Loans Receivable for Federal Entities and Related Interest

Receivable Serviced by **BPD** as of September 30, 2002 (OIG-03-022); and **FMS**' FY 2002 and 2001 Schedules of Non-Entity Assets, Non-Entity Costs, and Custodial Revenue, also known as Treasury Managed Accounts (OIG-03-021). With respect to the Treasury Managed Accounts, the IPA also provided a letter to FMS on information technology related issues (OIG-03-043).

Additionally, an IPA examined **BPD**'s assertions pertaining to schedules and notes for selected trust funds. The schedules related solely to the functions performed by BPD's Trust Fund Management Branch as custodian of the following Trust Funds' monies and investments: Federal Supplementary Medical Insurance; Federal Hospital Insurance; Highway; Airport and Airway; Hazardous Substance Superfund; Leaking Underground Storage; and Oil Spill Liability. The IPA concluded that the BPD's assertions were fairly stated and there were no instances of noncompliance with laws and regulations. (OIG-03-023)

Financial Related Reviews

During the semiannual reporting period, our office performed other financial related reviews pursuant to statute or other requirements, as discussed below:

- **Treasury Payments for DC Water and Sewer Services.** The District of Columbia (DC) Public Works Act of 1954 (P.L. 83-364), as amended, requires that bureaus make timely payments for DC water and sewer services. The Consolidated Appropriation Act of 2001 (P.L. 106-554) requires the Inspector General to submit a quarterly report to the Committees on Appropriations of the House of Representatives and Senate analyzing the promptness of payment with respect to the water and sewer services furnished to the Treasury by the District of Columbia. We performed certain agreed-upon procedures in evaluating the Department's compliance with the law. For the first and second quarters of FY 2003, we noted no exceptions. (OIG-03-005 and OIG-03-053)

- **Treasury's Annual Reporting of Drug Control Funds.** Beginning in 1998, Treasury agency participation in the Organized Crime Drug Enforcement Task Force (OCDETF) program was funded through a separate appropriation, known as Interagency Crime and Drug Enforcement (**ICDE**) within the Treasury. OCDETF was created in 1982 to mount a comprehensive law enforcement effort to dismantle sophisticated drug trafficking and money laundering organizations, and other related criminal enterprises.

  We reviewed the following management assertions included in the **ICDE**'s FY 2002 Annual Accounting of Drug Control Funds as required by law: (1) the obligations reported by budget decision unit were the actual obligations from the bureaus' accounting system of record for these budget decision units; (2) the methodology used to calculate obligations of FY 2002 budgetary resources by function and decision unit was reasonable and accurate; (3) the drug methodology disclosed in the report was the actual methodology used to generate the Table of FY 2002 Drug Control Obligations; (4) data presented was associated with obligations against a financial plan that properly reflects all revisions; and (5) the financial plan fully complied with all Fund Control Notices issued by the Director under 21 U.S.C. 1703 (F) and the Office of National Drug Control Policy (ONDCP) Circular section on budget execution.

The Annual Accounting, including the assertions made, was prepared pursuant to 21 U.S.C. 1704 (d) and the ONDCP

Circular *Drug Control Accounting*. Based on our review, nothing came to our attention that caused us to believe that management's assertions included in the Annual Accounting were not fairly stated, in all material respects, based on criteria set forth in the ONDCP Circular. (OIG-03-050)

We also reviewed the following management assertions included in **Customs**' Annual Reporting of FY 2002 Drug Control Funds as required by law: (1) the methodology used to estimate drug enforcement related obligations and full time equivalents was reasonable and accurate, (2) the methodology described in the Submission was used to prepare the estimates contained in the report, and (3) no changes were made to Customs' financial plan that required ONDCP approval. Customs' annual reporting, including the assertions made, was prepared pursuant to 21 U.S.C. 1704 (d) and the ONDCP Circular *Drug Control Accounting*. Based on our review, nothing came to our attention that caused us to believe that management's assertions were not fairly stated in all material respects based on the requirements set forth in the ONDCP Circular. Responsibility for future review of assertions made by Customs' management in the annual reporting of drug control funds has transferred to the DHS OIG. (OIG-03-051)

Information Technology Audits

BPD's Role In Treasury's Public Key Infrastructure Initiatives

BPD's effort leading Treasury's Public Key Infrastructure (PKI) technology initiatives has been significant. This technology can facilitate and simplify the delivery of products and services by providing electronic approaches to processes that have historically been paper-based.

We reviewed BPD's management of its PKI implementation to determine whether it was effective and found that BPD had not fully developed documentation needed to effectively manage this technology. Specifically, BPD's Certificate Policy Statement (CPS), which defines the practices and procedures utilized in conducting services and operations within a PKI, had not been updated to include the conduct of independent reviews and audits that would determine whether discrepancies exist in current operations. Without an updated CPS there is an increased risk that security controls associated with BPD's PKI can be circumvented and the integrity of web transactions can be jeopardized.

BPD management agreed with our finding and concurred with our recommendation to update the CPS to include procedures for the performance of independent reviews and audits. BPD is currently in the process of implementing corrective action. (OIG-03-009)

Controls Over Secret Service's Law Enforcement Data Need Improvement

The use of law enforcement data is vital to the missions of several Treasury bureaus, including the Secret Service. Secret Service had not established adequate controls to ensure the security and integrity of its law enforcement data.

We recommended a number of improvements to controls over the security and integrity of this data with which management concurred. Audit follow-up is the responsibility of DHS. (OIG-03-002)

Improving Treasury's Internal Operations

ATF Needs To Strengthen System Security And Controls For Its Law Enforcement Data

OIG auditors determined that ATF had not established effective automated system security and integrity controls necessary to protect its law enforcement data. ATF agreed with our findings and recommendations for improved controls and has taken steps to implement the recommendations. Audit follow-up for ATF's law enforcement activities is the responsibility of Justice. (OIG-03-061)

Inadequate System Security And Internal Controls Over Law Enforcement Data At FinCEN

FinCEN has not established adequate security and integrity controls over its law enforcement data. Bureau management agreed with our findings and recommendations, and has completed a number of corrective actions and is in the process of implementing the others. (OIG-03-007)

Security Vulnerabilities Pose Risks To BEP's Network And Systems

We identified security vulnerabilities that may compromise BEP's network and computer systems leaving them open to misuse and attacks. We used two commercial off-the-shelf tools to check for vulnerabilities in BEP's network services, operating system configurations, file and user permissions, routers, e-mail, servers, and applications. The bureau's network and systems are integral parts of BEP's mission support structure. An attack on BEP's network and computer systems could be detrimental to the manufacturing of U. S. financial securities, U.S. postage stamps, and other security documents.

We provided BEP and Department management with reports generated by the tools that detailed the specific vulnerabilities detected and the actions needed to address the vulnerabilities. We recommended that BEP continue to prioritize and address vulnerabilities detected in its systems to reduce risks and threats to assets, infrastructure, and information. In addition, we recommended that the Department continue to work with BEP management to prioritize and address the vulnerabilities detected in the bureau's telecommunication devices. (OIG-03-070)

Program Audits And Evaluations

BEP's Controls Over Background Investigations Need To Be Improved

The security aspects of BEP's mission require that areas of greatest vulnerability receive the greatest scrutiny. In January 1999, BEP implemented its new Personnel Security Policy for Positions in Vulnerable Areas, which superseded a 1996 policy. The 1996 policy limited full background investigations to persons who had access to finished products such as currency and stamps. The current (1999) policy sets forth an additional number of areas designated as vulnerable and applies to employees with access to areas including finished and unfinished products. BEP's Personnel Security Division has the responsibility for performing background investigations and maintaining data files. Since 1988, the Personnel Security Division has maintained its data of background investigations on a database called the Employee Suitability System (ESS).

We found that the ESS had inaccurate social security numbers and multiple records that needed to be deleted or archived. In addition, the ESS did not produce status reports that showed the collective number of open cases, the number of employees who have certain levels of security clearances (high risk, moderate risk, low risk), and the number of cases that are outstanding/pending investigation. We also observed that the BEP database is not currently designed to permit easy reconciliation with BEP's Office of Human Resources roster because of automation problems and incorrect data. In addition, the Personnel Security Division did not timely remove former employees from its current database. Although the 1999 policy designated more positions as high risk, we still found employees with moderate risk background investigations working in high-risk areas. There was also a backlog of open cases.

We recommended that BEP conduct a bureau wide self-assessment to improve its background investigations procedures and to address the problems we found. BEP's management agreed with our findings and recommendations and is in the process of implementing corrective actions. (OIG-03-004)

Customs' Purchase Card Program

As a cost-cutting measure, in December 1993, the Treasury Department directed all bureaus to begin using purchase cards for small purchases. Purchase cards are similar to personal credit cards, and are used to buy products and services with less paperwork involved than processing individual requisitions through the traditional procurement process. Credit card limits are issued to a cardholder with a transaction maximum and a maximum for aggregate monthly transactions. The Department mandated that the bureaus provide their employees with the necessary training and written procedures.

Customs established a Purchase Card Program that is responsible for administering and maintaining a Purchase Card System. Along with the Department's Directive, Customs has issued its own directive and purchase card manual. At the time of our audit, Customs had already issued 1,318 cards to its 20,693 employees, or about 6.4 percent of the Customs' workforce.

We found that, in general, the Customs Purchase Card Program was well planned and well administrated and that purchase cards are being used for their intended purpose. We reviewed five percent of a year's transactions and did not find any instances of fraud or abuse in the sample transactions. We also found that Customs had a system in place to ensure that payments to the contract vendor for the purchase card were on time so as to take advantage of the purchase card rebate. In addition, the Purchase Card Program performs random audits on cardholders and the purchase card is an area in the Self-Inspection Program. Both of these functions contribute to the internal controls of the overall program.

However, we did find areas where the program could be improved. Specifically, approving officials were not always reviewing supporting documentation (i.e. receipts and invoices) for purchase card transactions in conjunction with the reconciliation statement. This occurred because Customs did not include a formal step for documentation review as part of the approving official's responsibility in the purchase card process. We also found that cardholders and approving officials were not reconciling statements on time.

We recommended that Customs: (1) revise purchase card guidance regarding the approving official's responsibilities, and (2) ensure timely reconciliation and approval of statements. Customs management, in its response to our report, indicated that corrective action was being taken. Audit follow-up is the responsibility of DHS. (OIG-03-057)

Improving Treasury's Internal Operations

OCC Purchase Card Usage At The Western District and Headquarters

We reviewed OCC Headquarters and its Western District to determine whether OCC had appropriate controls over its Government Purchase Card program and ensured that purchase cards were used only for their intended purpose. During the audited period, OCC had 192 cardholders nationwide with over 9,500 transactions amounting to over $5.6 million. OCC headquarters accounted for 86 cardholders with over $2.2 million in transactions, and the Western District had 16 cardholders for over $900,000 in transactions.

We found that the OCC had adequate written policies and procedures over the use of the Government Purchase Cards. These procedures included sufficient internal controls to prevent and detect improper card usage. However, we found that prescribed policies and procedures were not always followed and that these deviations were frequent and extensive. In addition, post reviews and the primary control to detect deviations were seldom completed or exceeded prescribed review cycles. In reviewing 1,619 transactions for a sample of 24 cardholders, we found purchases that were not properly supported, approvals were unjustifiably made, and errors went undetected. Although we did not find that any of these deviations entailed large dollar items or indicated abuse, we concluded that the audited locations were more than moderately vulnerable to fraud, waste, and abuse.

Furthermore, we found that OCC used the purchase card as a primary payment mechanism and did not limit payments to small purchases as commonly used by other agencies. In some instances, these payments entailed large and recurring payments that included a 1.25% service fee charge per payment. We estimated that OCC paid about $11,000 in these service fees over a 28-month period. We questioned whether usage of this card feature was cost effective when compared to effecting payment through the Treasury (which would cost less than a dollar per payment).

We made eight recommendations aimed at enhancing the controls and usage of OCC purchase cards. Meanwhile, OCC resumed its internal audit program over checks paid relating to credit card purchases. The Agency Program Coordinator will provide reminders to cardholders and approving officials of the documentation that must be retained in support of the purchase card transactions. (OIG-03-031)

Treasury Departmental Offices' Control Over Computers Needs To Be Improved

We audited DO's control over computers as part of a request from a member of the Senate Finance Committee that our office conduct an assessment of Treasury's inventory practices regarding its stock of firearms, computers, and other items that might compromise the public's safety, national security or ongoing investigations. In this regard, we performed a series of audits of Treasury bureaus' controls over such property, most of which we completed during the last semiannual period. Sensitive property at DO included computers only. DO had written guidance, directives, and procedures for managing and safeguarding computers. DO also required reporting of all lost or stolen computers. However, we noted that DO did not conduct a periodic physical inventory of all its computers and we were unable to verify the number of computers reported lost or stolen during the audited period. The lack of a physical inventory provided inadequate internal control over loss or theft.

To address this issue, we recommended that a complete physical inventory of all computers be conducted on a periodic basis. The method for reporting lost or stolen computers should also be re-evaluated to ensure that all losses are reported to the proper authorities. Furthermore, the physical inventory should include periodic reconciliations of data relating to computers between the Chief Information Officer, Treasury Office of Security and Critical Infrastructure Protection, and OIG OI. Management concurred with the recommendations. (OIG-03-038)

Treasury Faces Challenges In Meeting Goals Established In The National Energy Conservation Policy Act

The National Energy Conservation Policy Act (NECPA), as amended by Energy Policy Act (EPACT) of 1992, requires Federal agencies to take action necessary to reduce energy consumption in Federal buildings by 20 percent between FYs 1985 and 2000. Executive Order 13123 adds additional energy reduction goals for FY 2005 and FY 2010.

In coordination with the Treasury Inspector General for Tax Administration (TIGTA), we reviewed Treasury's compliance with NECPA as amended by EPACT. TIGTA will report separately on the IRS. Our objective was to determine whether Treasury met the goal established for FY 2000 and whether Treasury is likely to meet the Administration's goals for FY 2005 and FY 2010.

Treasury, excluding the IRS, just missed its energy efficiency goal for standard buildings in FY 2000, and faces challenges in meeting the future goals established for FY 2005 and FY 2010. Treasury has made considerable efforts to improve energy efficiency in its industrial facilities. Despite these efforts, the improvement has not been sufficient.

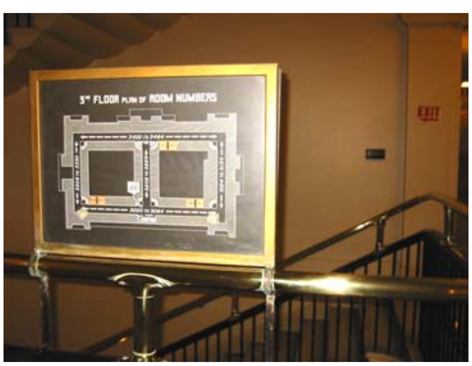
In response to our recommendations, management stated that the Office of Safety, Health, and Environment (OSHE) will engage the bureaus individually, and as a group, to fully identify the challenges they face in meeting the reduction goals. OSHE will also work with the bureaus to (1) identify projects that will assist them in meeting the goals, (2) identify funding sources for the projects, and (3) monitor progress. Specific action plans with goals and timeframes were outlined as well. (OIG-CA-03-003)

Treasury Employees Feel Safer With Greater Awareness Of Safety, Physical Security, Evacuation, And Continuity Of Operations Planning Procedures

Following the events of September 11, 2001, it has become increasingly important to improve emergency evacuation procedures and operations to enhance overall emergency preparedness. In an effort to find out employees' perceptions of emergency preparedness, we administered an online survey over a 3-week period from May 10 through May 31, 2002, to Treasury employees working in Washington, D.C., metropolitan area except for the IRS. The objective of this survey was to collect information on employee perceptions of safety, physical security, evacuation procedures, and continuity of operations planning (COOP), as well as to gain insight into employees' sense of personal safety while working in Treasury buildings. We administered the survey to 13,220 Treasury employees and received 3,283 responses.

The data from our survey revealed that Treasury employees had a range of knowledge regarding safety, physical security, evacuation procedures, and COOP issues. We found that the majority of employees located in Treasury buildings in the Washington, D.C. metropolitan area felt "very safe" or "somewhat safe" at their workplaces. In addition to their general feelings of safety and security, we asked employees to identify the potential workplace hazards and emergency situations that concerned them the most. Nearly 30 percent of Treasury employees noted "no present concerns." The others cited concerns pertained to building evacuation (about 26 percent of the respondents), potential terrorist activity (about 14 percent), general emergency situations (about 12 percent), and building security procedures (about 9 percent). The other respondents were most concerned with cluttered office areas, proximity to the White House, workplace violence, and "other" unspecified potential workplace hazards or emergency situations. Another finding worth noting was that Treasury employees knew very little about COOP. Just over half of the respondents (53.2 percent) were aware that their office had a COOP. However, employees in general were unaware of the specific details of the COOP.

Our summary report on the survey results was issued to the Acting Assistant Secretary for Management and Chief Financial Officer in April 2003. In its response, management indicates support for stronger emphasis on training and assessing results, and is developing specific actions to our recommendations. During this semiannual reporting period, we issued informational reports to the following bureaus summarizing the survey results as they pertained to those bureaus: ATF, Customs, FLETC, Secret Service, BEP, BPD, FinCEN, OCC, OTS, FMS, and Mint.
(OIG-CA-03-020)



Follow-up Review on Recommendations Concerning Treasury Enforcement Communications System (TECS) User Training

We conducted an evaluation to follow up on the corrective actions Customs implemented in response to two of the recommendations in our 1998 audit report, *Treasury Enforcement Communications System Users' Needs* (OIG-98-060)—whether TECS users were surveyed: (1) on their evaluations of the formal TECS training courses, computer-based training, and self-help tools; and (2) for comments of their specific training needs. Our review found these actions were taken.

We analyzed the responses to the survey Customs conducted of a group of 398 TECS users in October 1999. Customs personnel stated that necessary steps were taken to address TECS users' concerns and suggestions from their 1999 survey. In addition, we analyzed the responses to course evaluations that FLETC administered to 718 students who attended TECS training between May 1999 and June 2002.

Further program evaluation of TECS training is the responsibility of DHS.
(OIG-CA-03-006)

Treasury's Efforts To Implement An Integrated Document Management System

Integrated document management systems track the creation, location, version control, and workflow of documents, and ideally manages them during their complete life cycle based on their value to the agency's business. The increasing reliance on computer networks in the government means that more documents are being created and stored on computers. The Government Paperwork Elimination Act requires Treasury to prepare for the management of electronic documents across the entire Department. Treasury generates many documents/records electronically, such as electronic mail (e-mail) messages, word processing documents, spreadsheets, graphs, databases, compact disks, and web site pages. This can create software and hardware compatibility problems within the Treasury as well as in the public sector. Furthermore, Treasury's responsibilities are complicated by the decentralized nature of electronic records creation and control.

Since the former Acting Assistant Secretary for Management and Chief Information Officer had just completed a survey of common business services and that efforts were underway to identify and implement an integrated document management system (IDMS) department-wide, we limited our work to reviewing the responses already provided. Specifically we assessed the plans for a new system considering the current capabilities of the Treasury Control Management System (TCMS). In this regard, we reported that Treasury recognizes the need for an up-to-date electronic document/records management system. The CIO Council has formed a workgroup to research the needs and requirements of the bureaus and offices. The CIO Council will recommend an IDMS for Treasury-wide implementation. (OIG-CA-03-001)

Investigative Activities

Two Former Mint Employees Indicted For Theft of Sacagawea Mule Coins – Update

On June 13, 2002, as a result of an investigation conducted by the OI and previously reported, two former Mint employees were indicted on charges of conversion of government property and witness tampering. On February 12, 2002, one former employee pled guilty to conversion of government property and was sentenced to 6 months home detention, 5 years probation, 100 hours of community service, ordered to pay a fine of $5,000, and ordered to pay a special assessment of $100. The other former employee failed to appear for arraignment and a bench warrant was issued. Efforts to locate and arrest the other employee continue.

Obverse

Deli Owner Pleads Guilty

On July 19, 2002, as a result of a joint investigation by Treasury OIG, the Department of Labor and the Secret Service, a Philadelphia, PA deli owner was indicted on one count of bank fraud involving forged and uttered U.S. Treasury checks, totaling $140,053, from the Philadelphia Financial Management Center. On January 15, 2003, the deli owner entered a plea of guilty to conversion of government property, and aiding and abetting. Sentencing was scheduled for April 15, 2003.

Former BEP Contractor Agreed To Civil Settlement

In August 2001, an investigation determined that a contractor, who had previously been debarred from contracting with the Federal government for a period of 3 years for bribing city officials, continued to contract with Federal agencies. These agencies included the BEP and Western Currency Printing Facility, Fort Worth, Texas. The contractor was indicted on mail fraud and wire fraud charges for inflating his company's Department of Labor Workman's Compensation insurance rates. The indictment was subsequently dismissed and the subject agreed to a civil settlement of $450,000. The United States Attorney's Office, Eastern District of Texas, determined that the BEP would receive over $168,000, as part of the settlement. The settlement should be finalized in late February 2003.

Improving Treasury's Internal Operations

BPD Attorney Pleads Guilty

In September 2002, a joint investigation conducted by OIG and the Federal Bureau of Investigation determined that several individuals were involved in a high-yield investment "Ponzi" scheme. A cooperating defendant reported that he had paid $15,000 to a senior counsel with the BPD for providing them information by "vetting" potential high yield investments. The attorney was considered an "expert" in the field. The attorney also used his law enforcement contacts to help the cooperating defendant to recover two million dollars that was allegedly to be used in a high yield investment scheme. The joint investigation resulted in the indictment of the attorney for bribery and enhancing his government salary. The attorney entered a guilty plea to one count of enhancing his government salary, and is scheduled for sentencing in April 2003.

ATF Employee Made Unauthorized Cash Withdrawals With Government Credit Card -- Update

Following an OIG investigation, an ATF supervisor admitted to misusing her government-issued Citibank travel card. The investigation determined that the ATF employee made unauthorized cash advances totaling in excess of $11,000 over a 1-year period, and failed to fulfill financial obligations to Citibank relating to the unauthorized charges. ATF imposed a suspension without pay, a grade demotion to a non-supervisory position, and a directed reassignment. ATF also permanently revoked the employee's government credit card privileges.

Mint Employees Violate Civil False Claims Act -- Update

As previously reported, one of the three remaining Mint employees pending judicial action has agreed to a civil settlement of $17,931 as a result of his involvement in a scheme to defraud the U.S. Government. A joint investigation conducted by OI and the Department of Veterans Affairs disclosed that five Mint employees attending courses at a college in Oakland, CA, under a Veteran's Affairs Educational Assistance Program, conspired with instructors and other veteran students to receive passing grades, and collect VA benefits. One current Mint employee and one former Mint employee are awaiting sentencing.

Contractor Mislabeled Korean Auto Parts

An investigation conducted by OIG focused on the detection and interception of a shipment of mislabeled auto parts shipped from a Canadian contractor to a U.S. contractor. It was determined that the Canadian contractor had relabeled parts manufactured in Korea to indicate Canadian origin, and that the U.S. contractor under paid approximately $4,708 in duties. As a result of the investigation, the U.S. contractor subsequently paid the additional duties in full.

Mint Vendors Plead Guilty To Theft

As a result of an OI investigation, two Mint vendors, both coin dealers, have pled guilty to theft for their participation in a multi-year scheme with a former Mint employee to embezzle nearly $200,000 from the Mint. In furtherance of the scheme, the Mint employee directed Mint coin presentation boxes to be shipped from existing inventory to various vendors and, in return, the vendors paid him directly. Many of these coin presentation boxes have been recovered and additional prosecutions are pending. As a result of the joint effort by OIG, the United States Attorney's Office, and Mint Counsel, all of the money embezzled by the former Mint employee has been recovered.

Improving Treasury's Internal Operations

Departmental Employees Misused Government Computers To Send And Receive Pornographic E-mails

An OIG investigator identified several departmental employees who misused their government computers to send and receive numerous e-mail messages containing pornographic photographs and video clips.

These employees sent their pornographic e-mails to various other parties inside and outside the Department. This matter was brought to the attention of the OIG after one of the parties inadvertently sent a pornographic e-mail to a senior official in another organization. Disciplinary actions are pending.

Vendor Refunds Interest Earned From Misrouted Mint Payments – Update

Pursuant to a plea agreement between a Mint vendor and the U.S. Attorney's Office for the Eastern District of Pennsylvania, the vendor remitted to the government $26, 483 which represents interest he ostensibly earned while holding Mint funds in the amount of $1.2 million dollars that had been erroneously routed to him. The $1.2 million had been recovered early on in the investigation and was previously reported.

Coin presentation boxes

Customs Employees Misused Government Vehicles and Improperly Stored Government Issued Firearms

An OIG investigation determined that four Customs Special Agents traveled in Government-owned vehicles to a restaurant/bar to consume alcoholic beverages after completing a surveillance operation. Three of the Agents admitted to driving the government vehicles after consuming alcoholic beverages. The other Agent, who was a passenger, admitted to consuming alcoholic beverages also. Three of the Agents also admitted to storing their Government-issued firearms in the trunk of the government vehicles, in violation of Customs' policy. The remaining Agent kept his firearm in his personal possession. The three senior Special Agents received suspensions without pay for at least 30 days. The Agent riding as a passenger received a suspension without pay mitigated to 3 days.

Three Customs Senior Managers Disciplined For Failing To Follow Policy

An OIG investigation disclosed that a Group Supervisor, a Resident Agent in Charge, and the Special Agent in Charge of the Customs Office of Investigations failed to notify the Office of Internal Affairs, as required by Customs' policy, that four Special Agents traveled in Government-owned vehicles to a restaurant/bar to consume alcoholic beverages, after completing a surveillance operation.

The Group Supervisor was suspended without pay for 10 days, the Resident Agent in Charge resigned in advance of proposed disciplinary action, and the Special Agent in Charge was suspended without pay for 15 days.

Overseeing The Management Of The Nations' Revenue And Public Debt

Improved Management Of Customs Automated Commercial Environment (ACE) Business Process Reengineering Needed

The development of ACE is a significant and multifaceted effort that is critical to the long-term success of Customs mission. ACE is planned to be a customer-oriented, account-centric process that provides real-time secure access to internal and external information for travel and trade. The vision is for the Federal government to provide a "single window" for the trade to file the information required for all Federal border cargo regulations. This will reduce the burden on the trade by eliminating redundancy and simplifying the filing process. The objective of the audit was to determine whether Customs' commercial processes were appropriately reengineered prior to ACE software development.

Customs' high-level reengineering effort provided a baseline for the development contractor to initiate process development. However, we found that improved management of the reengineering process was needed in three areas. First, there was insufficient detail to allow the e-Customs Partnership to manage work and for Customs to measure the quality of contract deliverables. E-Customs Partnership is a coalition of contractors, led by IBM Global Services, developing ACE. A detailed Integrated Allocation Matrix can better define expectations, control shifts in processes, and track legacy systems that will be eliminated or changed. Second, the Customs Management Office (CMO) web portal was not available to all contractor and CMO employees. The portal will allow Customs and contractor employees to review the status of work and communicate information related to ACE development. Third, a multi-agency reengineering effort has not been performed to establish requirements for integrating International Trade Data System functionality into ACE.

We also brought two other issues were brought to Customs management's attention. There were indications that improvements were necessary in the staffing, utilization, and management of Customs' subject matter experts. Also, there were indications that the aggressive ACE schedule was affecting the quality of work products.

Customs concurred with the three recommendations made to improve the management of the reengineering of business processes. Customs has taken steps to require the contractor to prepare and maintain an Integrated Allocation Matrix and to provide Customs and contractor employees with a functional CMO web portal. Customs also began to gather system requirements from other agencies participating in ACE. Audit follow-up is the responsibility of DHS. (OIG-03-058)

Enhanced Controls Could Prevent Improper Payment Of Customs Drawback Claims

Drawback is a refund of Customs duties, fees, or taxes paid on imported merchandise that is subsequently exported or destroyed. In FY 2001, drawback payments were about $403 million. Drawback regulations were revised in 1998. Customs, accordingly, established procedures to expedite the processing of drawback claims, established a criteria-based selectivity system designed to indicate the level of review for drawback claims, and established penalty procedures. We performed an audit to determine whether drawback controls were adequate to prevent improper payments.

We found weaknesses in Customs processing of drawback claims in three areas that could result in claims being overpaid. While we did not find substantial improper claims payments or integrity concerns, we identified problems with system controls and claims review, inconsistencies in the use of the criteria-based selectivity system, and problems with inspection, targeting, and certain drawback-related procedures that increased the potential for improper payments to occur.

First, in our review of drawback claims, we found one improper claim payment of $30,000 that occurred due to weak system controls and claims review. The system allowed for override of an error message when this refund calculated by the drawback specialist did not agree with the amount entered in the system for claim liquidation; other compensating controls designed to prevent improper payments did not work in this instance. While this was the only improper payment found, we believe the potential exists for other claims to be overpaid until controls are strengthened.

Second, we found that Customs personnel did not consistently use the criteria-based drawback selectivity system because Customs did not formalize procedures on how to use this system. For example, we found instances in which problems identified by the drawback specialist had not been entered into the criteria-based selectivity system, and as a result the claims had undergone only minimal review. Also, Customs did not apply consistent criteria for denied claims, or ensure that criteria were specific enough to identify that aspect of the claim that required attention. Further, Customs did not provide official written guidance to the drawback offices on how to take corrective actions for an invalid drawback claim, or on how to pursue penalties.

Third, we found problems with the targeting of drawback claims for inspection and with certain other procedures that, taken together, increased the potential for improper payments. Inspectors told us that they did not always review criteria or consult with drawback specialists to target merchandise for examination. In addition, controls were weak over the exportation of drawback merchandise, and there was no assurance that goods were exported or that the exported goods were the ones for which drawback had been claimed.

We made a number of recommendations to correct the noted problems, including reinforcing supervisory controls over claim payments, establishing system controls when developing ACE to prevent error messages in the drawback system from being bypassed, identifying claimant criteria that are significant enough to warrant review of all unliquidated claims for these parties, and enhancing or clarifying procedures and guidance in a number of areas. Customs concurred with the recommendations and has taken or planned corrective action. Audit follow-up is the responsibility of DHS. (OIG-03-026)

Assessing Law Enforcement Programs

Customs Agreed To Improve The Security, Inspection, And Targeting Of Vessel Containers At U.S. Seaports

Seaport security and the cargo that enters the United States' seaports have become prominent issues in the last few years. Coverage has been extensive in the media and Congressional Committees have devoted much attention the issue. All have expressed concern for the serious threat represented by the possibility of smuggling weapons of mass destruction (WMD), implements of terrorism, narcotics, and other contraband into the country via containerized shipping.

One of the major challenges for Customs involves the increasing number of vessel container arrivals. Almost 90 percent of the vessel containers processed in FY 2002 came through the top 10 major seaports. A total of about 6.8 million vessel containers, shipped from foreign countries, arrived at U.S. seaports in FY 2002. This represents a 27 percent increase in container traffic from the prior year. Another concern for Customs is the need to process this volume of workload in such a manner as to properly facilitate trade while safeguarding our seaports from possible terrorist activities.

Cargo entering the port for inspection

We performed audits at five ports and issued a separate report for each. Nearly two thirds of the nations' cargo are received at these ports we reviewed. The five ports were: Los Angeles/Long Beach (OIG-03-041), New York/Newark (OIG-03-066), Charleston (OIG-03-063), Philadelphia (OIG-03-060), and Port Everglades (OIG-02-090, which was reported in our previous semiannual report).

Our findings at the ports indicated that additional actions were necessary to tighten security, intensify the inspection of vessel containers, and improve the targeting process. We found that: (1) vessel containers were not properly secured; (2) examinations and the recordings of those results could be improved, and the inspection process could be enhanced through increased utilization of examination tools; and (3) targeting high-risk containers could be improved.

We made several recommendations to local Customs officials who were responsive to these recommendations and initiated immediate corrective action. However, the commonality of conditions identified at the ports visited indicated that closer oversight and direction by Customs Headquarters management was needed to ensure that vessel containers were effectively secured, inspected, and targeted for inspection. Accordingly, we issued a summary report to Customs outlining our findings and the actions required attention from a national perspective. Customs management agreed with our recommendations addressing these issues on a national level, and is taking corrective actions. Audit follow-up is the responsibility of DHS. (OIG-03-074)

Customs' Railcar Inspection Program At Port Huron, MI, Needs Further Improvement

In response to a prior OIG audit, Customs agreed to implement changes to its rail interdiction activities along the Northern Border. Our review of the current rail inspection program in Port Huron, Michigan, showed that corrective actions were implemented. However, the railcar inspection program at this major port of entry was not adequately targeting or inspecting high-risk shipments.

Customs' long-range plans are to significantly increase inspections through the use of non-intrusive inspection equipment. However, until this equipment is deployed, interim measures need to be taken to reduce the risk of contraband from entering the country through this port.

To address these issues, we made seven recommendations. Customs agreed with the recommendations and established target dates for completing corrective actions. Audit follow-up is the responsibility of DHS (OIG-03-071).

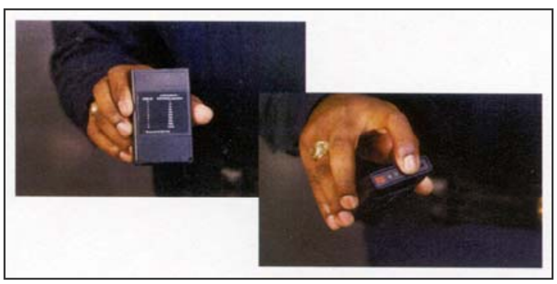
Customs Utilization Of Trace Detection Equipment

Trace detection technology makes use of the minute amounts of vapors given off and the microscopic particles left behind when narcotics and explosives contraband are packaged and handled. This technology provides Customs with the capability to screen and search in a non-intrusive manner for the trace quantities of narcotics and explosives on people, baggage, cargo, vehicles, containers, tickets, and identification cards. Prior to the events of September 11th, trace detection technology was utilized by Customs with an emphasis on narcotics interdiction.

Trace detection equipment was delivered to the field as part of the initial deployment on non-intrusive inspection equipment that was undertaken in the late 1990s per the *Customs' Five-Year Technology Plan.* The objective was to add this technology to the ports' arsenal of tools providing a "layered defense" to smuggling attempts. The ports had latitude to utilize the trace detection equipment where they felt it would be most effective.

Our review of trace detection equipment disclosed opportunities for Customs to utilize trace detection equipment in a more efficient and effective manner. Specifically, we noted improvements were needed in:
(1) management direction to ensure that the detectors were placed in locations most conducive to their use, (2) maintenance, and (3) inspector training. Customs concurred with our recommendations. Audit follow-up is the responsibility of DHS. (OIG-03-068)

Customs Deployment Of Radiation Detection Equipment



Personal radiation detection device

Customs has made progress since the terrorist attacks of September 11th, in improving detection of radioactive materials that may be smuggled into the U.S. at the ports of entry. Customs has deployed, or is in process of deploying, several different radiation detection devices to the ports of entry. These devices range from personal radiation detectors, which are somewhat limited and not very costly, to more sophisticated, capable, and costly portal radiation detection systems. Customs views these systems as complementary and each is viewed as valuable in its own right in detecting radioactive materials at the ports.

We believe, however, that Customs' radiation detection capability has been hindered because Customs has not developed a documented strategic plan for the acquisition and deployment of radiation detection equipment. In addition, Customs has not been collecting data on the usage or performance of this equipment in detecting illegally imported radioactive materials.

Customs concurred with our findings and recommendations and plans to have a draft strategic plan by September 2003. In addition, Customs is currently collecting data on significant detections made with the equipment. Audit follow-up is the responsibility of DHS. (OIG-03-073)

Examination Of International Mail For Contraband And Revenue

All international mail arriving for delivery in the U.S. and U.S. Virgin Islands is subject to Customs' inspection and release. Inspection is performed at Customs International Mail Branches (IMB). The 14 IMBs are located at, or close to, United States Postal Service (USPS) facilities. Mail is examined to prevent contraband or other illegal articles from entering the U.S. and to collect revenue on dutiable items. Customs screens the mail using visual inspection, x-ray equipment, x-ray equipment with mounted radiation detectors, personal radiation detectors, isotope identifiers, and detector dogs.

We found that Customs cannot guarantee that all mail arriving into the U.S. is properly transported, secured, and presented to the IMBs for examination. Many IMBs have not established adequate techniques to monitor the mail prior to its presentation to Customs.

The need to properly examine parcels is also important for identifying dutiable parcels in the mail. Customs often relies on values on mail declarations, which Customs found, during a mail revenue survey, are not always accurate. The results of a Customs mail revenue survey for FY 2001 showed that an estimated $184 million a year is uncollected based on values stated on the mail declarations, and an estimated $494 million per year is uncollected based on examination of the contents of the parcels.

Some IMBs have developed new targeting strategies using the results of the survey to detect dutiable parcels, and others are continuing to use their current methods. However, because of the lack of resources, the IMBs are at a disadvantage for identifying and collecting all the revenue.

Unsecured mail left on tarmac

To correct the problems above, we recommended that Customs: (1) examine the transportation process of all international mail and work with USPS to ensure mail is properly secured, (2) implement a plan for screening tools and detector dogs to be used at all of the IMBs, and (3) continue to work on a strategy to identify and collect all revenue due.

Customs concurred with our recommendations and will work with the USPS and other customs and postal administrations to improve mail examination procedures. Audit follow-up is the responsibility of DHS. (OIG-03-072)

The Customs National HAZMAT Program Needs To Be Strengthened

This audit was the third and final report in a series of audits Customs hazardous materials (HAZMAT) Program. The objective was to determine whether Customs had sufficient processes in place to ensure the safe and legal transport and inspection of cargo containing hazardous materials. Our first report provided recommendations for improving the HAZMAT Program at the Port of Brownsville (OIG-02-123) and our second report provided recommendations to strengthen the program at the Port of Houston (OIG-03-049).

We reported that Customs' management controls are not sufficient, HAZMAT training records were not adequately documented and maintained, and Emergency Action Plans at port facilities were missing or needed to improve required Occupational Safety and Health Administration elements.

Customs concurred with our recommendations and agreed to take corrective action including having the HAZMAT Headquarters Administrator and the Hazard Assessment Team personnel take a more active role in the HAZMAT Program activities at the Ports, and revising the HAZMAT Handbook. (OIG-03-065)

Implementation Of The Report Of International Transportation Of Currency Or Monetary Instruments (CMIR)

CMIR information is collected for use in criminal, tax or regulatory investigations or proceedings. Information collected may be provided to investigative officers and employees of Customs and to any other law enforcement and regulatory personnel in the performance of their duties. FinCEN administers the Bank Secrecy Act (BSA) of 1970, which includes implementing the Treasury regulatory requirements for CMIR-reported transactions. Customs, through its ports of entry, processes over 90 percent of the CMIR transactions. The remaining 10 percent of transactions are mailed to its headquarters office for processing.

We performed an audit to determine whether allegations concerning a backlog of CMIR transactions had merit. We also: (1) determined whether Customs and FinCEN established the appropriate internal control processes to effectively implement revisions to the CMIR form, (2) evaluated whether Customs has enhanced its data base system to accommodate changes to the revised form, and (3) assessed any accelerated efforts taken to alleviate the potential backlog of CMIR transactions.

We found that Customs had taken actions to address a backlog of over 200,000 CMIRs that had existed for over 18 months. The reported backlog was resolved by December 2001. Customs also executed an action plan in January 2002 to improve its internal controls over the CMIR processes and program. Some of the action plan items had been addressed at the time of the audit while others were in process at the end of our fieldwork. We believe once the action plan items have been completed, it should further enhance and improve the overall CMIR processes and program.

In addition, we found that CMIRs known as rejects were sent back to the ports because of deficiencies like incomplete forms, missing information, and missing signatures. As a result, some of the ports did not always comply with regulatory requirements for reporting. During our audit, Customs was addressing the controls and procedural action plan items associated with these deficiencies. Also actions were taken by Customs to accommodate required TECS database changes to facilitate capture of CMIR data into TECS.

During the review, we followed up on a 1999 OIG recommendation regarding the CMIR form. At that time we recommended that the form be revised to include certain travelers' checks, money orders, and foreign bank drafts as reportable monetary instruments. Through the coordinated efforts of Customs and FinCEN, a revised form was issued in April 2000.

Customs concurred with our recommendations to: (1) evaluate its current efforts to fund the CMIR program; (2) continue efforts to further improve overall CMIR program processes and the CMIR form; (3) assess more cost effective and operationally efficient methods for administering the program, including an automated integrated system; and (4) continue efforts with FinCEN to further streamline and improve the CMIR form. Audit follow-up is the responsibility of DHS. (OIG-03-062)

Assessing Law Enforcement Programs

Secret Service's Control Over Seized Property Needs Improvement

We audited the Secret Service's controls over seized property as a part of a request from a member of the Senate Finance Committee that we assess Treasury bureau inventory practices regarding their stock of firearms, computers, and other sensitive items. In this regard, we performed a series of audits of Treasury bureaus' control over such property, most of which we completed during the last semiannual period.

While the Secret Service had strong physical controls limiting access to seized property by non-Secret Service personnel, we noted, based on our observations at eight selected locations that it did not:
(1) fully control or document access to seized property by its personnel,
(2) package seized property in a way that made it easy to detect tampering or produce a complete and accurate physical inventory, (3) maintain complete, up-to-date seized property records, and (4) conduct appropriate physical inventories of seized property. These weaknesses increased the risk that items of seized property could be lost or stolen and decreased the likelihood that inventory differences would be timely detected. We made seven recommendations to improve controls over seized property. Audit follow-up is the responsibility of DHS. (OIG-03-013)

ATF's Implementation Of The Youth Crime Gun Interdiction Initiative (YCGII)

In July 1996, ATF announced YCGII to strengthen enforcement efforts against gun traffickers who supply firearms to youths. At the time YCGII began, homicides committed by young people with firearms had nearly tripled since 1985, and other types of gun related violence were on the rise. YCGII was first implemented in 17 pilot cities. There are now 50 cities participating in the program. YCGII has the following primary goals: (1) ensure all recovered crime guns are traced through ATF's National Tracing Center; (2) conduct research and analysis to determine community-wide patterns and trends; (3) produce an annual report for state and local authorities for use in making informed enforcement strategies, focused on the reduction of firearms violence and interdiction of firearms to age groups of concern; and (4) use this information to increase the effectiveness of enforcement efforts in the apprehension and prosecution of those who illegally possess and traffic firearms. In FY 2002, roughly 10 percent of ATF's annual budget ($85 million and 480 FTE positions) were appropriated for YCGII.

ATF National Tracing Center
Falling Waters, WV

We performed this audit to assess the corrective actions taken by ATF in response to our audit report issued in August 2000. (OIG-00-119). As a result of the prior audit, ATF agreed to: (1) provide additional guidance to field offices for improving communication between ATF and state and local police departments and (2) develop new performance measures that gauge YCGII's affect on trafficking of firearms to youths.

We concluded that ATF adequately implemented 6 of 9 recommendations from the prior audit, but needs to perform further work for 3 recommendations. Specifically, we found that field offices may not have received additional staffing as a result of their cities participation in the YCGII program, thus limiting the resources being devoted to YCGII activities. Additionally, ATF is developing performance measures that show YCGII's impact on youth crime, but these efforts are still ongoing. Related to performance measurement, we also noted that ATF's definition of what constituted a YCGII case was not clear and cases identified as YCGII varied between field offices. As a result, ATF could not ensure the accuracy of YCGII data.

ATF concurred with our findings and recommendations from this follow-up audit. ATF will continue to examine its staffing model to adjust them for crime rates and varying needs of the individual localities. ATF management stated that the performance measures are a work in progress and it will continue to refine performance measures to ensure accuracy in measuring YCGII efforts. Lastly, to ensure validity of information, ATF is developing a plan to sample and validate case/time data. Audit follow-up is the responsibility of Justice. (OIG-03-019)

Operations At ATF's Philadelphia Field Division

ATF field division offices conduct a variety of operations to implement the bureau's three main activities: reducing violent crime, collecting revenue, and protecting the public. We assessed whether ATF's Philadelphia Field Division was effectively carrying out its responsibilities in certain areas.

We found the Field Division did not always ensure licensees completed corrective actions required to close out noted firearms and explosives violations. Specifically, licensees' inspection files we reviewed did not contain sufficient documentation to support whether the licensee completed corrective action on 58 of 168, or about 35 percent, of the violations inspectors cited for the 42 compliance inspections we reviewed. About half of these violations pertained to discrepancies ATF inspectors noted on firearm transaction records maintained by Federal Firearms Licensees for firearms dispositions.

Additionally, Division personnel did not always comply with ATF guidelines for using the Government purchase card. Our review of purchase card transactions found several misuses of the purchase card, including two individuals who used another employee's card to make a purchase, employees who made several purchases prohibited by ATF, a cardholder who exceeded the $5,000 monthly purchase threshold, several cardholders who did not sign their monthly purchase card statements or purchase card receipts, and several receipts which did not provide a description of the items purchased.

Philadelphia Field Division management agreed with our recommendations, which included:(1) ensuring inspectors properly complete inspection reports that note violations with both a corrective action and completion date, (2) establishing Division-wide guidance for handling violations concerning firearm transaction records, and (3) taking action to ensure Division personnel comply with ATF purchase card guidelines. Audit follow-up is the responsibility of Justice. (OIG-03-067)

FLETC's Actions To Reduce A Material Weakness Associated With Operation Of Its Outdoor Dirt Berm Firing Ranges

The objective of the review was to determine whether the actions taken by the FLETC associated with the operation of its four outdoor berm firing ranges were sufficient to reduce hazardous environmental conditions from a material weakness to a "second tier" reportable condition. We found that FLETC made several modifications over the years to the dirt berm ranges to reduce the environmental and safety concerns associated with the operation of these ranges. Additionally, the overall firearms training environment has been improved. Accordingly, it is our opinion that the deficiency no longer rises to the level of a material weakness.

FLETC management plans to further remediate the outdoor dirt berm firing ranges by a newly revised target date of April 2005. Also, it concurred with our recommendation to establish an action plan to achieve the completion and any additional tasks associated with the remediation. Follow-up is the responsibility of DHS. (OIG-03-036)

Customs' Advance Passenger Information System Is A Valuable Enforcement Tool But Relies On Factors Outside Of Customs' Control

APIS provides airport inspectors from both the Immigration and Naturalization Service (INS) and Customs with biographical information on airline passengers and crewmembers from foreign countries. While initially a voluntary program, a November 2001 law now requires all carriers to provide this information. Customs is responsible for ensuring that air carriers comply with APIS requirements and Customs is authorized to issue penalties to airlines that do not comply.

APIS identifies individuals to intercept and examine. INS and Customs personnel intercept targeted passengers or crew for examination. We found concerns with the system that hindered Customs' enforcement efforts. We also noted that penalties for non-compliance were administered inconsistently.

Seizure/Arrest Categories	Number
Drug Related	122
Warrants	51
Trademark Violations	10
Check Fraud	1
Counterfeit money/checks	1
Failure to Declare	15
Child Pornography	1
Stolen credentials	3
Cuban merchandise/travel	11
Cigarette smuggling	3
Seized as Evidence	1
Illegal Alien	1
Seizures (details not available)	3
Grand Total	223

Number and type of APIS seizures and arrests from Jan 1 – Sep 15, 2002

To enhance enforcement efforts, we recommended that INS and Customs monitor the usefulness of APIS as an enforcement tool. Additionally, we recommended that Customs take a more uniform approach to enforcing compliance with APIS requirements. Customs has taken appropriate action to address these recommendations. Audit follow-up is the responsibility of DHS. (OIG-03-059)

Customs Enforcement Of Intellectual Property Rights

Intellectual property is defined as the exclusive ownership of an original product created from the work of individual artistic, inventive, and novel ideas. The Government provides protection to owners by allowing registration of these properties under copyrights, trademarks, and patents. These owners can also record their rights with Customs, who monitors imported and exported goods for possible violation of these rights. Registration records, along with other intellectual property information related to imports, reside in the Customs Automated Commercial System Intellectual Property Rights (IPR) Module used by Customs import specialists, inspectors, and other personnel involved with the enforcement of these rights.

We found that the IPR Module did not have accurate, complete, and reliable information to help Customs' field personnel identify IPR infringements.

Contributing to this problem was a recordation process that lacked a standard data input form and sufficient internal controls to prevent errors from occurring. In addition, we found that IPR Module data available to the public on the Customs Electronic Bulletin Board, accessible at Customs' web site, was unreliable. Our audit also disclosed that many employees had inappropriate access to IPR function codes that could allow them to add, change, or delete data within the IPR Module. This matter was discussed with IPR Branch officials, who took action to eliminate inappropriate access. Additionally, we found a lack of maintenance and accountability over the original files of IPR information.

Customs concurred with our recommendations to improve the management of the IPR Module. Audit follow-up is the responsibility of DHS. (OIG-03-027)

Enforcement Of Export Controls

This review was conducted in partnership with the OIGs at the Departments of Commerce, Defense, State, and the Central Intelligence Agency. The overall objective was to evaluate the adequacy and effectiveness of Treasury's export enforcement activities concerning the transfer of militarily sensitive technology to countries of concern, including efforts to (1) prevent the illegal export of dual use-items and munitions and (2) investigate and assist in the prosecution of export control violators.

We found that Customs has devoted limited resources to export enforcement. We identified a number of factors that impaired Customs' ability to effectively enforce export controls, some of which were beyond Customs' control. We also found that although Customs implemented planned corrective actions to address recommendations made in a 1999 OIG audit report regarding export enforcement, similar conditions still existed during our current review. Therefore, we believe that corrective actions taken were not always effective in correcting the deficiencies cited in the prior report.

We also found that the Office of Foreign Asset Control (OFAC) could benefit from better coordination with the State Department and Customs. We noted that Customs needs to keep OFAC apprised on the status of referred cases.

We made 11 recommendations to improve the effectiveness of Treasury's enforcement of export controls. DHS and Justice will have audit follow-up responsibility for recommendations pertaining to Customs and ATF, respectively. The Department will be responsible for recommendations directed at OFAC. (OIG-03-069).

Reliability Of Suspicious Activity Reports

A key component of the BSA requires financial institutions to file a Suspicious Activity Report (SAR) of any suspected violations and illegal acts, including money laundering, with FinCEN. FinCEN maintains a database of filed SARs that provide law enforcement agencies leads and/or an audit trail to investigate money laundering schemes and other illegal activities. The events of September 11th elevated the role of SARs as a means to combat terrorist financing. We initiated our review to profile the types of suspected illegal activities reported by national banks and savings associations. However, we deferred this review when a related matter came to our attention that warranted FinCEN's immediate attention. Our concern centered on the reliability of SAR data and its possible adverse effect on FinCEN's ability to meet its core mission related to BSA and the attendant money laundering enforcement programs.

Since the inception of SARs in 1996, over a half a million had been filed as of December 2000. Based on interviews with law enforcement agencies—primary SAR users—we determined that the SAR System would be more useful if it included more complete and accurate SAR data. Law enforcement agencies noted that some SARs lacked critical information, included inaccurate information, or were listed multiple times because financial institutions: (1) disregarded SAR filing instructions, (2) did not always understand the violations listed on the form, or (3) were concerned with personal liability.

Additionally, SARs may be filed on hard paper, magnetic tape or via the new Patriot Act Communication System. However, SAR data entry errors and omissions were not always corrected prior to entry into the SAR System. In this regard, FinCEN required only minimal data edits and data perfection routines, and generally did not follow up with institutions that reported erroneous filings. Some of the noted filing errors included missing key information such as the suspected violation, the responsible Federal regulator, and a narrative description of the suspected illegal activity. As a result, the SAR data did not always have all the critical information law enforcement agencies needed to investigate transactions or trace funds derived from illegal activities. We previously reported this problem in 1999, but our current review found that corrective actions had not been fully effective or implemented. Given this ongoing problem and the expanded types of institutions that would be subject to filing SARs in the future under the USA PATRIOT Act, we reported that FinCEN should consider reporting the SAR data reliability problems as a "material weakness" under the Departments' reporting requirements for the Federal Manager's Financial Integrity Act.

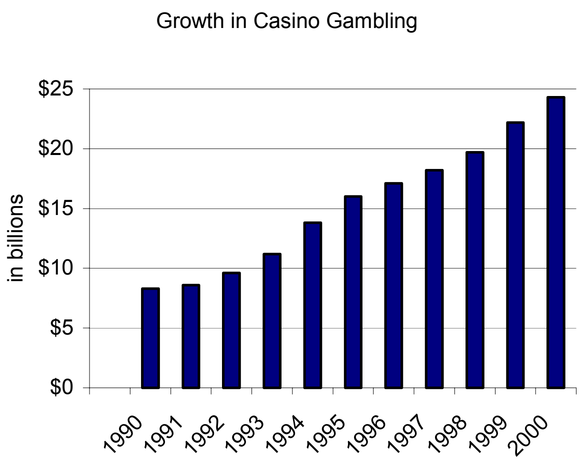
We recommended that FinCEN, in coordination with the IRS Data Center and Federal bank regulators: implement procedures to increase SAR editing, require mandatory data fields be completed, and provide feedback to financial institutions and regulators. FinCEN also needs to revise the SAR filing instructions, or by other means, address problems with narrative write-ups. We also recommended that FinCEN address the problem with duplicative and Internet SAR filings. FinCEN officials acknowledged the ongoing problems with the reliability of SAR data. FinCEN management concurred and provided proposed enhancements to the Federal bank regulatory agencies. FinCEN also committed to have an overall implementation plan by June 2003. This plan will consider ways to improve industry outreach efforts. The plan will further evaluate approaches to handle duplicate SARs and data perfection routines. (OIG-03-035)

FinCEN's Efforts To Deter And Detect Money Laundering In Casinos

Money laundering is defined as moving illegally obtained funds through financial institutions to make the funds appear unrelated or untraceable to the illegal activities from which they originated. The law requires financial institutions to maintain certain records and report on certain types of financial transactions. While BSA was initially limited to financial institutions, the BSA was amended in 1985 to include casinos with gross gaming revenue of $1 million. In calendar year 2000, it was estimated that casino gross revenue totaled about $26 billion.

FinCEN depends on regulatory partners to help it administer the BSA. For casinos, FinCEN works in partnership with the IRS to determine whether casinos are complying with the BSA. The only exception is for casinos in Nevada, which are monitored by Nevada's Gaming Control Board (GCB). When IRS examiners find casinos that have not complied, they refer their casino examination reports to FinCEN for civil penalty consideration.

As of August 2001, we found FinCEN had not obtained or reviewed adequate information from the IRS and the State of Nevada to be able to provide assurance that casinos were complying with the BSA. selection rationale and the number of casinos IRS examined.



Also, FinCEN officials responsible for overseeing compliance could not provide us information about Nevada casino compliance. They were unaware that GCB officials had been sending quarterly reports to a FinCEN employee

We also found FinCEN did not process IRS casino examination referrals in a timely and consistent manner. Specifically, we reviewed 28 IRS casino examination referrals FinCEN resolved after January 1999. We found it took FinCEN more than 3 years to resolve 7 of the 28 referrals. FinCEN resolved 7 referrals with warning letters or no enforcement action when, historically, FinCEN had penalized casinos for BSA violations.

In addition, we found FinCEN had not finalized the suspicious activity report by casino (SARC) regulations it proposed in 1998. Also, the database FinCEN uses for proactive targeting did not contain more than 4 years' worth of currency transaction reports by casino, which reduced the value of the analysis.

To more effectively administer casino compliance with the BSA, we recommended FinCEN: (1) take a number of actions to improve the information received from its regulatory partners, (2) clarify enforcement actions when non-compliance occurs, (3) subject casinos to SAR reporting requirements, and (4) improve the analysis of casino BSA information. FinCEN management generally concurred with our findings and recommendations and implemented or is in the process of implementing corrective actions. For example, FinCEN issued the SARC regulations in September 2002 that require casinos to report suspicious financial transactions beginning in March 2003. (OIG-03-001)

Customs Faces Staffing Challenges Along The Northern Border

To review staffing challenges faced by Customs due to heightened security following the events of September 11th, OIG evaluators visited 30 Northern border ports of entry in January 2002. Using a structured questionnaire, interviews were conducted with Customs inspectors and a limited number of other Federal agencies' employees. We also observed and photographed the conditions at the ports/crossings, while traveling along approximately 3,200 miles of the Northern border.

We found that Customs used several approaches to address staffing challenges along the Northern border. Specifically, Customs temporarily assigned inspectors, activated seasonal and part-time employees, and utilized staff from other Federal and state agencies. Customs officials, however, expressed concern about the length of time it takes to hire and place full-time inspectors. In addition, several unique conditions exist that impact staff assigned to the Northern border such as the remoteness of some ports of entry, limited housing, and extreme winter weather conditions.

We also found that clarification of staffing requirements is needed during the time of heightened alert levels in terms of defining a port of entry, officers' responsibilities while on duty, and physical jurisdictional boundaries. Customs management concurred with the three recommendations and has taken planned corrective actions. Follow-up is the responsibility of DHS. (OIG-CA-03-002)

Policies, Procedures, And Training Related To Racial And Ethnic Profiling – A Comparative Review

We performed a comparative review of policies, procedures, and training to prohibit racial and ethnic profiling by Treasury law enforcement bureaus. The objectives of the review were to determine whether the bureaus: (1) published written policies and procedures which set out the bureau position on racial and ethnic profiling for inspectors and agents, (2) distributed the policy, (3) provided related training to inspectors and agents, and (4) periodically reviewed practices and any citizen complaints to ensure compliance. To accomplish our objectives, we met with officials from the ATF, Customs, and Secret Service to obtain information on racial and ethnic profiling policies, procedures, and training. We learned the Administration requested that the Department of Justice study the policies and practices of Federal law enforcement agencies regarding the use of race in law enforcement decision-making. Therefore, we obtained the bureaus' responses to the study, and reviewed the policies, procedures, and general training information provided.

As a general observation, we would have expected the three bureaus to have similar policies and training to prohibit racial and ethnic profiling in their law enforcement activities. While ATF and Customs had specific policies and training addressing racial and ethnic profiling, the Secret Service considered its more general policies and training on EEO and ethical conduct sufficient to prohibit racial and ethnic profiling. Separate informational reports were issued to the Commissioner of Customs and the Director of Secret Service. (OIG-CA-03-009 and OIG-CA-03-009)

Law Enforcement Bureaus Claim Information Sharing Within Treasury To Be Adequate

Following the terrorist attacks of September 11th, an area of crucial importance to improve counter terrorist operations was information sharing, both among Treasury law enforcement agencies, and between law enforcement agencies and the national intelligence community (NIC). We met with representatives from ATF, Customs, Secret Service, FinCEN, and the Department's Office of Intelligence Support (OIS). The objectives of these meetings were to: (1) determine how Treasury law enforcement bureaus share information, and whether opportunities existed to improve the flow of information between Treasury law enforcement bureaus, and (2) identify the mechanisms through which Treasury law enforcement bureaus share information with NIC. We used a structured questionnaire for these interviews.

Under the first objective, agency representatives reported no substantial problems in sharing information among Treasury law enforcement bureaus. For the second objective, our results were included as part of a study of intelligence sharing between the Federal law enforcement community and NIC conducted by a working group of the Intelligence Community Inspectors General (ICIG). For the Treasury offices and bureaus involved in the sharing of intelligence information, we reported on their mission, the information that they typically shared, and the agencies with which they share it. The working group reported its findings, which included our information, to the full ICIG in April 2002.

FinCEN and OIS remain with the Treasury while the other law enforcement bureaus were divested pursuant to the HSA. (OIG-CA-03-012)

Working To Maintain Confidence In The Nation's Banking System

We are responsible under the Federal Deposit Insurance Act (FDIA) section 38(k), 12 USC 1831o(k), to conduct a "material loss review" if a failed insured financial institution regulated by OCC or OTS has caused a material loss to a deposit insurance fund. A loss is considered material if it exceeds $25 million or 2 percent of an institution's total assets. An FDIA-mandated review essentially requires us to: (1) ascertain the cause(s) of the insured institution's failure; (2) assess OCC's or OTS' supervision of the failed institution; and (3) where applicable, recommend how such failure might be avoided in the future. As a part of the material loss review, we also assess OCC's or OTS' implementation of 12 USC 1831 o, *Prompt Corrective Action*.

FDIA requires that we report on our review within 6 months after notification of the material loss by the Federal Deposit Insurance Corporation (FDIC). Our report must be provided to the regulator (OCC or OTS), the Comptroller General of the United States, and upon request, to any member of Congress.

During this semiannual reporting period, we completed two material loss reviews of institutions regulated by OCC. The failed institutions were: (1) NextBank, N.A., located in Phoenix, Arizona; and (2) Hamilton Bank, N.A., located in Miami, Florida. Following is a discussion of these reviews.

Material Loss Review Of NextBank, National Association

On February 7, 2002, OCC closed NextBank after determining that unsafe and unsound practices had substantially dissipated assets and that insolvency was imminent without Federal assistance. NextBank was OCC's first Internet-only credit card bank that operated primarily through an internet-platform rather than a traditional storefront operation. The bank's capitalization reflected the high-tech enthusiasm at the time, but the bank's internet-based operations had been based on an unproven business model that could not generate earnings or profits. In less than two and half years, NextBank grew six fold from $300 million to over $2 billion in managed assets, never turned a profit, and failed. NextBank's failure is projected to cost the FDIC $300 to 350 million, making it the most costly failure in 2002. With its failure occurring in under 3 years, NextBank possibly has the distinction of being the fastest bank failure in decades.

We found that NextBank's failure could be attributed primarily to improperly managed rapid growth that led to unsustainable levels of credit risk. This risk was magnified by a major switch in business focus from prime to sub-prime credits. Ultimately the emerging credit risk resulted in losses and capital depletion. Even the credit risk reduction technique of securitizing assets had been partially offset by NextBank's practice of providing recourse on sold assets, and NextBank's problems were obscured by deficient accounting practices.

OCC's supervisory performance was mixed. Sanctions taken in late 2001 and early 2002 appeared timely and appropriate. However, OCC's initial examinations were partly hampered by resource constraints, which appeared to have delayed OCC's detection of NextBank's actual risk profile, embedded asset problems, and unsafe banking practices. Left without an effective enforcement action in place after OCC surfaced the initial signs of unsafe banking practices, NextBank continued its uncontrolled growth to large and costly levels. Besides the noted supervisory areas of concern, we also found that OCC appeared to have been unable to invoke certain pre-and post operating conditions when NextBank first started operating in 1999. This was as a result of NextBank's owners seemingly taking advantage of OCC's different application procedures for granting banks ownership through a new charter versus acquisition of an existing bank charter. Furthermore, the lack of adequate supervisory oversight of the NextBank's holding company also highlighted a vulnerable supervisory gap between OCC and the holding company's functional regulator.

Our report included a number of recommendations aimed at the following courses of action: (1) enhancing certain regulatory matters dealing with credit card banks, (2) refining certain examination and enforcement processes, (3) reviewing for potential Prompt Corrective Action violation, (4) reviewing Change-in-Control applications, and (5) reviewing the oversight of unsupervised national bank parent companies. OCC concurred with our findings and recommendations and committed to formulating action plans detailing the steps to be taken to implement the recommendations. (OIG-03-024)

Hamilton's initial core business was trade finance in emerging markets in the Caribbean Basin and in Central and Latin America. During the mid-1990s, senior management saw the potential for rapid growth and high earnings. To fund planned growth, the bank's parent holding company issued an initial public offering (IPO) in 1997. After the IPO, the holding company was required to make periodic public disclosures of financial results as required by the Securities Exchange Commission for publicly traded companies. To satisfy the demands of its shareholders, the bank was under pressure to show strong earnings. The IPO and resulting pressures led to a change in the bank's mission and credit philosophy for which the bank did not have the supporting expertise or infrastructure.

The bank grew significantly over the years from $22 million in assets in 1988 to $1.7 billion in 2000. The greatest asset growth occurred between 1996 and 1998, from $755 million to $1.7 billion.

Material Loss Review Of Hamilton Bank

OCC closed Hamilton on January 11, 2002, after finding that the bank was undercapitalized and suffered from deteriorating asset quality, poor earnings, a high level of non-performing loans, and sharply declining capital levels. At the time of Hamilton's closing, it had $1.3 billion in recorded assets. FDIC initially estimated that Hamilton's closure would cost the Bank Insurance Fund between $350 and $500 million. As of June 30, 2002, FDIC adjusted the estimated cost of Hamilton's closure to between $175 million and $225 million, taking into account the recovery of international loans and asset sales.

Hamilton's closure in January 2002 occurred after the board of directors and management failed to adequately respond to OCC's supervisory and enforcement actions to rehabilitate the bank. While the immediate cause of Hamilton's closure was due to unsafe and unsound practices, the root causes of the bank's closure can be attributed to the following: (1) aggressive growth and asset concentrations in foreign markets, (2) increased credit risk due to weak underwriting, (3) inadequate risk management systems and controls, and (4) an ineffective board and non-responsive management.

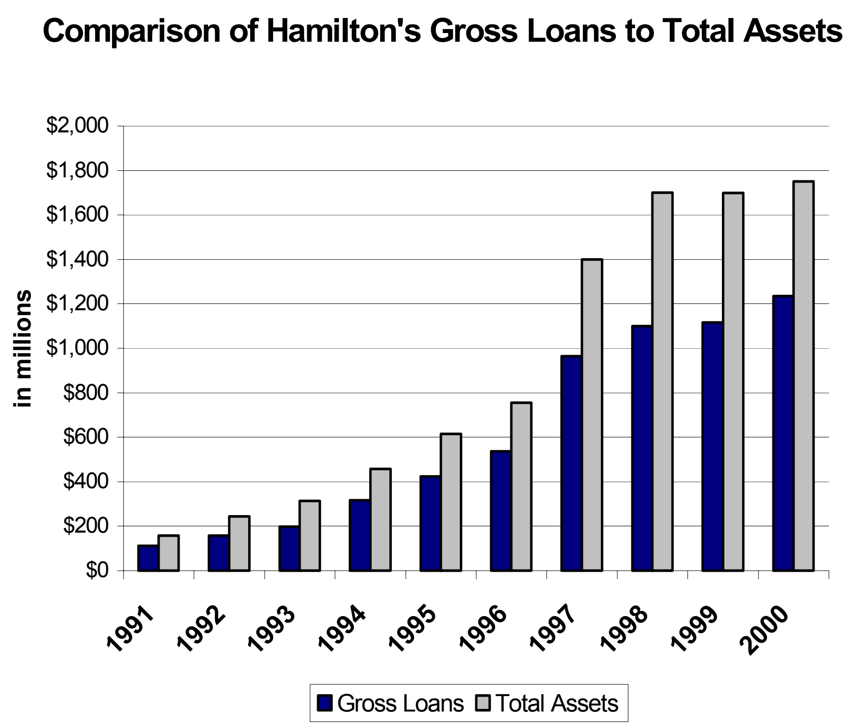
OCC's on-site examinations and resulting enforcement actions could have been more aggressive between 1992 and 1997. OCC did not fully identify or address the bank's management weaknesses or unsafe lending practices until the bank had already established a base of problem loans.

OCC's 1998 examination identified significant accounting issues but OCC did not follow-up on these matters until 10 months later. In addition, OCC issued a Safety and Soundness Notice following the 1998 examination. However, OCC did not adhere to its policies regarding the follow-up procedures to determine compliance with the notice.

From September 1999 to the January 2002 closing, we concluded that OCC's supervision and enforcement actions of Hamilton were generally adequate, but by then it was too late given the issues identified in the earlier years, including the buildup of problem loans and a well-established pattern of non-responsiveness by management. If these management and lending problems had been fully addressed sooner, OCC's ratings of Hamilton may have been different and may have resulted in earlier, more forceful supervision and enforcement actions.

OCC completed an internal quality assurance review (Lessons Learned Review) of Hamilton prior to our report. We believe many of the review's recommendations from the Lessons Learned Review are implemented, (2) improve certain aspects of the Lessons recommendations for improvement address most of our findings. However, our report contained additional recommendations aimed at enhancing the supervisory and examination process. Specifically, we recommended that OCC: (1) ensure the Learned Review process, (3) develop or revise policies and procedures to ensure examiners promptly review significant capital injections to determine whether the capital resources are managed and invested in accordance with the financial institution's business plan and in a safe and sound business manner, (4) reassess examination guidance regarding actions to be taken when examiners encounter unusual accounting transactions that warrant further investigation, and (5) establish controls to ensure examiner follow-up on bank compliance with enforcement actions in a timely manner. OCC concurred with the findings and agreed to implement the recommendations. (OIG-03-032)

Working To Maintain Confidence In The Nation's Banking System



Hamilton grew its assets throughout the 1990's. Total assets increased from $157 million to $1.3 billion in just six years—from the beginning of 1992 to the end of 1997. Growth rates during that time ranged from a low 23 percent in 1996 to a high of 77 percent in 1997, the year of the bank's IPO. The rapid expansion of the loan portfolio in relation to the total assets is indicated in the above chart.

Our Work – The Numbers

Summary of OIG Activity Between April 1, 2002 and March 31, 2003		
	4/1/02 – 9/30/02	10/01/02 – 3/31/03
OIG Activity	Number / $ Amount	Number / $ Amount
Reports Issued (Audits & Evaluations)	54	92
Reports Issued & Oversight Reviews (Investigations)	61	60
Regulation and Legislation Reviews	21	3
Disputed Audit Recommendations	0	0
Significant Revised Management Decisions	0	0
Management Decision in Which the IG Disagrees	0	0
Instances Where Information Was Refused	0	0
Number of Hotline Calls	2,453	828
Monetary Benefits (Audit)		
a) Questioned Costs	$1,383,000	$2,560,000
b) Funds Put to Better Use	$6,030,000	$1,482,000,000
c) Revenue Enhancements	$6,759,000	13,440,000
Total Monetary Benefits (Audit)	$14,172,000	$1,498,000,000
Monetary Benefits (Investigations)		
a) Fines/Restitutions	$237,734	$391,031
b) Recoveries	$0	$231,191
c) Savings/Cost Avoidance	$200,000	0
Total Monetary Benefits (Investigations)	$437,734	$622,222

Administrative Sanctions
October 1, 2002 - March 31, 2003

		Offices of Internal Affairs and Inspection			
	OIG	ATF	Customs	Secret Service	Total
Personnel actions	13	0	228	16	257
Suspensions and/or debarments of contractors	0	0	0	8	8

Prosecutorial Actions
October 1, 2002 – March 31, 2003

		Offices of Internal Affairs and Inspection			
	OIG	ATF*	Customs	Secret Service	Total
Cases pending prosecutorial decision at start of period	0	0	7	8	15
Cases referred to prosecutorial authorities	8	2	7	4	21
Cases accepted for prosecution	4	1	5	2	12
Cases declined	4	1	2	2	9
Cases pending prosecutorial decision at end of period	0	0	7	8	15
Successful prosecutions **	5	0	10	2	17

* Prosecutorial Actions 10/1/02 – 1/24/03
** Includes those found guilty by a Federal or state court, accepted for pretrial diversion agreements by the Department of Justice, or granted plea bargaining agreements.

Our Work – The Numbers

Audit Reports with Questioned Costs for the Period October 1, 2002 to March 31, 2003 (Dollars in thousands)	Divested Bureaus		Remaining Treasury Bureaus		Total		Unsupported Costs
	No. of Reports	Questioned Costs	No. of Reports	Questioned Costs	No. of Reports	Questioned Costs	
For which no management decision had been made by beginning of reporting period	0	$0	12	$2,417	12	$2,417	$0
Which were issued during the reporting period	0	$0	2	$143	2	$143	$0
Subtotals	0	$0	14	$2,560	14	$2,560	$0
For which a management decision was made during the reporting period	0	$0	6	$387	6	$387	$0
dollar value of disallowed costs	0	$0	0	$0	0	$0	$0
dollar value of costs not disallowed	0	$0	6	$387	6	$387	$0
For which no management decision has been made by the end of the reporting period	4	$752	4	$1,421	8	$2,173	$0
For which no management decision was made within six months of issuance	2	$610	4	$1,421	6	$2,031	$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 with Recommendations that Funds be Put to Better Use for the Period October 1, 2002, to March 31, 2003
(Dollars in thousands)

Total for Divested Bureaus and Remaining Treasury Bureaus

Category	Number of Reports	Total	Savings	Revenue Enhancements
For which no management decision has been made by the beginning of the reporting period	1	$6,030	$6,030	$0
Which were issued during the reporting period	2	$1,489,410	$7,410	$1,482,000
Subtotals	3	$1,495,440	$13,440	$1,482,000
For which a management decision was made during the reporting period	3	$1,495,440	$13,440	$1,482,000
dollar value of recommendations agreed to by management	3(a)	$1,493,195	$11,195	$1,482,000
based on proposed management action	3(a)	$1,493,195	$11,195	$1,482,000
based on proposed legislative action	0	$0	$0	$0
dollar value of recommendations not agreed to by management	1(a)	$2,245	$2,245	$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 six months of issuance	0	$0	$0	$0

Our Work – The Numbers

Continued

Audit Reports with Recommendations that Funds be Put to Better Use for the Period October 1, 2002, to March 31, 2003 (Dollars in thousands)				
Divested Bureaus				
For which no management decision has been made by the beginning of the reporting period	0	$0	0	$0
Which were issued during the reporting period	1	$1,482,000	0	$1,482,000
Subtotals	1	$1,482,000	0	$1,482,000
For which a management decision was made during the reporting period	1	$1,482,000	0	$1,482,000
dollar value of recommendations agreed to by management	1	$1,482,000	0	$1,482,000
based on proposed management action	0	$1,482,000	0	$1,482,000
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 six months of issuance	0	$0	0	$0

Audit Reports with Recommendations that Funds be Put to Better Use for the Period October 1, 2002, to March 31, 2003 (Dollars in thousands)				
Remaining Treasury Bureaus				
For which no management decision has been made by the beginning of the reporting period	1	$6,030	$6,030	$0
Which were issued during the reporting period	1	$7,410	$7,410	$0
Subtotals	2	$13,440	$13,440	$0
For which a management decision was made during the reporting period	2	$13,440	$13,440	$0
dollar value of recommendations agreed to by management	2(a)	$11,195	$11,195	$0
based on proposed management action	2(a)	$11,195	$11,195	$0
based on proposed legislative action	0	$0	$0	$0
dollar value of recommendations not agreed to by management	1(a)	$2,245	$2,245	$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 six 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. Two audits were performed by DCAA.
(a) One report was partially agreed to and partially not agreed to.

Our Work – The Numbers

Contract Audits Completed (Dollars in Thousands)						
	Pre-Award Audits		Costs Incurred Audits		Other Contract Audits	
Entity	Number Completed	Funds to be Put to Better Use	Number Completed	Questioned Costs	Number Completed	Questioned Costs
ATF	0	$0	1	$0	0	$0
BEP	1	$7,410	0	$0	0	$0
Customs*	0	$0	2	$142	0	$0
Mint	0	$0	1	$0	0	$0
Totals	1	$7,410	4	$142	0	$0

All Treasury bureau requests for pre-award, cost incurred, and other contract audits are referred to the OIG. We have the option to perform the audits, refer the audits to Defense Contract Audit Agency (DCAA) or other Government audit agencies, or contract with an IPA. DCAA performed the above 5 contract audits, which questioned approximately $7.6 million in Treasury contractor costs. Contracting officers agreed to savings and disallowed costs of approximately $10.4 million, including amounts that were questioned prior to October 1, 2002. An additional $2.1 million in potential monetary benefits, including amounts that were questioned prior to April 1, 2002, are awaiting completion of negotiations with the contractors.

*Audit follow-up is the responsibility of DHS.

Management Decisions with which the Inspector General is in Disagreement
There were no such decisions this period.

Reports with Pending Management Decisions Undecided for Over Six Months as of March 31, 2003 (Dollars in thousands)					
			Questioned Cost Amount		
Title and Date Issued	Bureau	Report Number	Divested Bureaus	Remaining Treasury Bureaus	Total
Costs Incurred Under Contract TOS-91-31 for Calendar Year 1991, 3/12/96 b/	DO	OIG-96-042		$5	$5
Contractor's FY Ended December 31, 1992 through 1994, Applicable to Contracts TOS-91-31 and TOS-94-25, 2/25/98 b/	DO	OIG-98-045		$562	$562
Incurred Costs for Contractor's FY Ended December 31, 1997, 8/23/99 a/	Customs	OIG-99-108	$197		$197
Incurred Cost for Contract TOS-92-20 for FY 1997, 1/7/00 b/	DO	OIG-00-030		$584	$584
Costs Claimed Under Contract TSW-87-0228, 10/1701 c/	DO	OIG-01-010		$270	$270
Direct and Indirect Costs and Rates Incurred Under Contract TC-94-027 for Contractor's FY 1998, 2/2/01 a/	Customs	OIG-01-037	$413		$413
Totals		6 Reports	$ 610	$1,421	$2,031

Management decision refers to the evaluation by management of the findings and recommendations included in a report and the issuance of a final decision.
a/ Contract negotiations have not yet been held or completed.
b/ Contract negotiations are currently on going.
c/ Awaiting contract modification to close contract.

Our Work – The Numbers

Significant Unimplemented Recommendations as of March 31, 2003		
Report Number	Issue Date	Report Title/Potential Monetary Benefits and Recommendation Summary
OIG-95-130	9/95	***Audit of Customs FY 1994 Financial Statements*** Improve and integrate core financial systems by including a "customer-based" accounts receivable subsidiary ledger; identify the modifications necessary to the general ledger systems to capture all financial transactions as they occur. Audit follow-up is the responsibility of DHS.
OIG-99-011	11/98	***U.S. Secret Service's FY 1997 Financial Statements*** Ensure that the seized property system captures all seized property data necessary to generate a complete analysis of changes in seized and forfeited property. Improve controls over property and equipment by ensuring that the exception reports are researched timely and proper disposition determined. Improve cut-off procedures for year-end closing by ensuring that documents processed after the year-end for reimbursable agreements are reviewed so that accounts receivable are properly reflected at year-end. Audit follow-up is the responsibility of DHS.
OIG-99-123	9/99	***Bureau of Alcohol, Tobacco and Firearms Controls Over Tax Free Spirit Exports*** Amend 27 CFR to include specific timeframes for Distilled Spirits Plants to submit documents that support claimed exports and additional guidance defining export evidence.
OIG-00-036	2/00	***Customs' Performance Data for Commercial Activity*** Implement COMPEX sampling for pedestrians and passengers arriving by vessel, bus, private aircraft and at small airports. Audit follow-up is the responsibility of DHS.
OIG-00-111	7/00	***United States Customs Service Has Undercharged Couriers for the Cost of Inspector Services*** Amend regulations to increase the computational charge to reflect the cost of services provided, and ensure staffing at courier locations is appropriate. (Two recommendations). Audit follow-up is the responsibility of DHS.
OIG-01-014	11/00	***Review of Treasury Computer Security Plans*** Update system security planning guidance, ensure that periodic reviews are conducted of the bureau security plans, correct identified DO system vulnerability plans and identify all existing and newly implemented DO Systems. (Two recommendations)
OIG-01-019	11/00	***Alcohol, Tobacco and Firearms Needs to Improve its Controls Over Tax-Free Tobacco Exports*** Establish controls to ensure Tobacco Unit specialists to properly monitor open notices of removal listed in the pending files.
OIG-01-025	12/00	***Review of Treasury's Infrastructure Protection Program*** Ensure that funding and resources are made available to implement PDD 63, and effective oversight of PDD 63 activities is implemented. (Two recommendations)
OIG-01-026	12/00	***Review of Surcharges from the Sale of Commemorative Coins*** Ensure that the Mint's implementation of Activity Based Costing (ABC) provides equitable and cost effective methods for allocating G&A costs.
OIG-01-035	1/01	***Report on the US Custom's Change Control Procedures*** Revise the draft standard Operating Procedures for Operating System Support to include guidance for hardware changes and emergency changes; document security approval of applicable changes, and establish test plans for changes. (Three recommendations.) Audit follow-up is the responsibility of DHS.
OIG-01-039	2/01	***Information Technology: The Financial Management Services Change Control Process Needs Improvement*** Update system and user documentation to reflect system changes; ensure major FMS systems have current accreditations, and properly control tapes. (Three recommendations)
OIG-01-045	2/01	***United States Customs Service's Fiscal Years 2000 and 1999 Financial Statements*** Recommendations made in prior years relating to core financial systems, drawback controls, compliance measurement programs, and in-bond shipment controls are reaffirmed. Audit follow-up is the responsibility of DHS.
OIG-01-063	3/01	***Review of Controls Over Entry Summaries Subject to Anti-dumping or Countervailing Duty*** Ensure that the procedures requiring supervisors verify that applicable entries have been liquidated and follow-up with field personnel on all unliquidated entry summaries open 4 months after liquidation. Audit follow-up is the responsibility of DHS.

Our Work – The Numbers

OIG-01-066	4/01	***Improvements Needed in the Administrative of the ATF's Certificate of Label Approval (COLA) Program*** The ATF Director should ensure that the information in ATF's COLA/Formula Modernization System is updated timely and accurately to better manage the COLA.
OIG-01-071	5/01	***Change Management Controls Lack Departmental Oversight*** Issue guidance to address systemic information technology problems, develop oversight to include guidance on internal security review programs, and schedule regular visits to each bureau and ensure compliance with issued guidance.
OIG-01-076	2/02	***U.S. Mint's Fiscal Years 2000 and 1999 Financial Statements*** Ensure that the CIO and CFO review, update, and maintain risk assessments and security plans.
OIG-01-077	6/01	***Protecting the Public: Bureau of Alcohol, Tobacco, and Firearms' Investigative Case and Time Data Needs Improvement*** Establish a method to track all dates for opening, closing, and re-opening, and re-closing of individual cases. Audit follow-up is the responsibility of Department of Justice.
OIG-01-084	1/02	***Narcotics Interdiction: Customs Management Action Needed to Ensure Benefits of Non-Intrusive Inspection Technology are Fully Realized*** Ensure that the effectiveness of non-intrusive inspection equipment is measured, ensure quality controls are established so that seizure data is accurate, ensure that Customs better collects and analyzes non-intrusive inspection utilization data, issue a notice emphasizing the need and importance of accounting for Busters on a routine basis, further discuss problems associated with the installation and deployment of large non-intrusive inspection systems, ensure that a formal planning process be adopted for deployment and installation of the major non-intrusive inspection systems, and ensure that the existing policy requiring Personal Radiation Detectors use be followed, and justify the non-use of Personal Radiation Detectors. Audit follow-up is the responsibility of DHS.
OIG-02-016	1/01	***Bank Secrecy Act: OCC BSA Examination Coverage of Trust and Private Banking Services*** Improve the examination monitoring process used by management to ensure adequate oversight of BSA examinations covering trust and private banking services.
OIG-02-020	12/01	***Customs is Not Collecting All Revenue Due From International Mail*** Ensure that the data exchange system is approved and established as soon as possible. Audit follow-up is the responsibility of DHS.
OIG-02-033	1/02	***Remote Video Inspection System Deployment Goals Have Not Been Achieved*** Ensure that Customs establishes Standard Operating Procedures and enters into an updated Memorandum of Understanding with the Immigration and Naturalization Service. Audit follow-up is the responsibility of DHS.
OIG-02-065	3/02	***Export Licensing Process: Progress Has Been Made But Better Cooperation And Coordination Are Needed*** (multi-bureau) OFAC should pursue a partnership agreement with Customs/Census that will provide direct access to Automated Export System (AES) and stipulate the data that will be accessible by OFAC personnel. In accordance with the Automation Initiative and the Government Paperwork Elimination Act, Customs should coordinate with the State Department to ascertain the feasibility of eliminating the paper Shipper's Export Declaration (SED) requirement. Customs should continue its efforts to encourage participation in AES with agencies involved in the export licensing process. Audit follow-up is the responsibility of DHS.
OIG-02-066	3/02	***Stronger Fund Controls are needed in the Puerto Rico Office of Special Agent-in-Charge*** Ensure that the frequency and amount of Puerto Rico Trust Funds reprogrammed, to include the justification for these actions, comply with Customs guidelines; update the budget manual to clarify the internal controls over the Puerto Rico Trust Fund. Audit follow-up is the responsibility of DHS.
OIG-02-071	3/02	***Financial Management: Audit of the United States Mint's FY's 2001 and 2000 Financial Statements*** Information system general controls and control at the application level need improvement.

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

Recent Reports

The following OIG reports were issued during the period of October 1, 2002 through March 31, 2003. Each entry in the list contains the name of the report, report number (prefixed by "OIG" for audit reports or "OIG-CA" for evaluation reports, issue date, and if applicable, the amount of revenue enhancements **(R)**, savings **(S)**, and questioned costs **(Q)**.

Improving Treasury's Internal Operations

Secret Service, Information Technology: Controls Over Secret Service's Law Enforcement Data Needs Improvement, OIG-03-002, 10/3/02

BEP, General Management: The Bureau of Engraving and Printings Controls Over Background Investigations Need to be Improved, OIG-03-004, 10/16/02

Treasury, Financial Management: Treasury Payments for Water and Sewer Services Provided by the District of Columbia for the First Quarter of Fiscal Year 2003, OIG-03-005, 10/16/02

Departmental Offices, Information Technology: Treasury's Efforts To Implement An Integrated Document Management System, OIG-CA-03-001, 10/22/02

FinCEN, Information Technology: Controls Over the Financial Crimes Enforcement Network's Law Enforcement Data Need Improvement, OIG-03-007, 10/23/02

BPD, Information Technology: The Bureau of the Public Debt's Certificate Policy Statement Should Be Updated, OIG-03-009, 10/24/02

Treasury, The Department of the Treasury's Fiscal Years 2002 and 2001 Financial Statements, OIG-03-014, 11/15/02

Mint, Financial Management: The United States Mint's Schedule of Custodial Gold and Silver Reserves as of September 30, 2002 and 2001, OIG-03-015, 11/13/02

OCC, Audited Financial Statements of the Office of the Comptroller of the Currency for Fiscal Years 2002 and 2001, OIG-03-016, 11/18/02

Number of OIG Reports Issued (By Office/Bureau) October 1, 2002 – March 31, 2003	
Office/Bureau	Number
ATF	9
BEP	5
BPD	6
Customs	27
Department-wide or Multi-Bureau	7
Departmental Offices	9
FFB	2
CDFI Fund	1
FinCEN	4
FLETC	2
FMS	6
Mint	3
OCC	5
OTS	2
Secret Service	4
Total	92

OTS, Audited Financial Statements of the Office of Thrift Supervision for Fiscal Year 2002, OIG-03-017, 11/18/02

Departmental Offices, Audited Financial Statements of the Office of DC Pensions for Fiscal Years 2002 and 2001, OIG-03-018, 11/19/02

Departmental Offices, Audited Financial Statements of the Departmental Offices For Fiscal Years 2002 and 2001, OIG-03-020, 11/21/02

FMS, The Financial Management Service's Fiscal Years 2002 and 2001 Schedules of Non-Entity Assets, Non-Entity Costs and Custodial Revenue, OIG-03-021, 11/21/02

BPD, Report on the Schedule of Loans Receivable from Federal Entities and Related Interest Receivable Serviced by the Treasury Bureau of the Public Debt at September 30, 2002, OIG-03-022, 11/25/02

BPD, Report on the Bureau of the Public Debt Treasury Trust Fund Management Branch Schedules and Notes for Selected Trust Funds for the Period October 1, 2001 to September 30, 2002, OIG-03-023, 11/25/02

Recent Reports

Treasury, Information Technology: Treasury's Continued Progress In Achieving Compliance With the Federal Financial Management Improvement Act, OIG-03-025, 12/12/02
FFB, Audited Financial Statements of the Federal Financing Bank for Fiscal Years 2002 and 2001, OIG-03-028, 12/4/02
BPD, Report on Controls Placed In Operation and Tests of Operating Effectiveness for the Treasury Bureau of the Public Debt Federal Investments Branch for the Period October 1, 2001 to September 30, 2002, OIG-03-029, 12/6/02
BPD, Report on 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, 2001 to September 30, 2002, OIG-03-030, 12/6/02
OCC, OCC: Purchase Card Usage at The Western District and Headquarters, OIG-03-031, 12/16/02
Customs, Financial Management: Report on Internal Control Over Financial Reporting of the U.S. Customs Service For Fiscal Year 2002, OIG-03-033, 12/16/02
Departmental Offices, Financial Management: Audited Financial Statements of the Treasury Forfeiture Fund for Fiscal Years 2002 and 2001, OIG-03-034, 12/17/02
Departmental Offices, Financial Management: The Exchange Stabilization Fund's Fiscal Years 2002 and 2001 Financial Statements, OIG-03-037, 12/20/02
Departmental Offices, Protecting the Public: Treasury Departmental Offices' Control Over Computers Needs to be Improved, OIG-03-038, 12/20/02
FMS, The Financial Management Service's Fiscal Years 2002 and 2001 Schedules of Non-Entity Government-wide Cash, OIG-03-039, 12/23/02
FMS, Management Letter for Fiscal Year 2002 Audit of Schedule of Non-Entity Government-Wide Cash **(LOU),** OIG-03-040, 12/24/02
FMS, Management Letter for Fiscal Year 2002 Audit of Schedule of Non-Entity Assets, Non-Entity Costs and Custodial Revenue, OIG-03-042, 12/27/02
FMS, Management Letter for Fiscal Year 2002 Audit of Schedule of Non-Entity Assets, Non-Entity Costs and Custodial Revenue **(LOU)**, OIG-03-043, 12/27/02
ATF, Financial Management: Internal Control Over Financial Reporting of the Bureau of Alcohol, Tobacco and Firearms for Fiscal Year 2002, OIG-03-044, 1/2/03
ATF, Management Letter for Fiscal Year 2002 Examination of Internal Control Over Financial Reporting at the Bureau of Alcohol, Tobacco and Firearms, OIG-03-045, 1/2/03
BEP, Financial Management: Audited Financial Statements of the Bureau of Engraving and Printing for Fiscal Year 2002, OIG-03-046, 1/7/03
FFB, Management Letter for Fiscal Year 2002 Audit of the Federal Financing Bank Financial Statements, OIG-03-047, 1/7/03
Treasury, General Management: Treasury Faces Challenges in Meeting Goals Established in the National Energy Conservation Policy Act, OIG-CA-03-003, 1/10/03
CDFI Fund, Audited Financial Statements of the Community Development Financial Institutions Fund for Fiscal Years 2002 and 2001, OIG-03-048, 1/21/03
Departmental Offices, Financial Management: Review of Assertions Included in the Interagency Crime and Drug Enforcement's Fiscal Year 2002 Annual Accounting of Drug Control Funds, OIG-03-050, 1/24/03
Customs, Financial Management: Review of Assertions Included in the U.S. Customs Service's Annual Reporting of Fiscal Year 2002 Drug Control Funds, OIG-03-051, 1/29/03
ATF, Financial Management: The Bureau of Alcohol, Tobacco and Firearms EDP General and Selected Application Controls **(LOU)**, OIG-03-052, 1/29/03
Treasury, Financial Management: Treasury Payments for Water and Sewer Services Provided by the District of Columbia for the Second Quarter of Fiscal Year 2003, OIG-03-053, 1/31/03

Recent Reports

Treasury, Agreed-Upon Procedures for the Department of the Treasury Fiscal Year 2002 Federal Intragovernmental Activity and Balances, OIG-03-054, 2/4/03
Treasury, Agreed-Upon Procedures for the Department of the Treasury Fiscal Year 2002 FACTS 1 Account Groupings Worksheets, OIG-03-055, 2/6/03
Customs, Treasury's General Management: Customs Purchase Card Program, OIG-03-057, 2/5/03
ATF, General Management: Bureau of Alcohol, Tobacco and Firearms Employees Vary in Perceptions of Building Security, Continuity of Operation Planning, and Personal Safety, OIG-CA-03-004, 2/10/03
Customs, General Management: Customs Employees Feel Safer When Enhanced Security Procedures Are in Place, OIG-CA-03-005, 2/11/03
Customs, General Management: Follow-up Review on Recommendations Concerning TECS User Training, OIG-CA-03-006, 2/21/03
FLETC, General Management: Greater Washington, D.C. Area Federal Law Enforcement Training Center Respondents Feel Safe at Their Workplace, OIG-CA-03-010, 2/27/03
Secret Service, General Management: Although Secret Service Employees Vary in Building Security and Continuity of Operation Planning, Most are Confident of Personal Safety, OIG-CA-03-011, 2/26/03
ATF, Information Technology: The Bureau of Alcohol, Tobacco and Firearms Needs to Strengthen System Security and Controls for Its Law Enforcement Data **(LOU)**, OIG-03-061, 2/27/03
Customs, Financial Management: The United States Customs Service EDP General and Selected Application Controls **(LOU)**, OIG-03-064, 2/28/03
BEP, General Management: Although the Majority of Bureau of Engraving and Printing Employees Lack Knowledge of Continuity of Operation Planning and Procedures, Building Security Procedures and Signage Promoted Feelings of Safety, OIG-CA-03-013, 3/13/03
BPD, General Management: Most Bureau of the Public Debt Survey Respondents Felt Safe and Were Generally Aware of Issues Affecting Their Personal Safety, Building Security, and Continuity of Operation Planning, OIG-CA-03-014, 3/13/03
FinCEN, General Management: Financial Crimes Enforcement Network Employees Vary in Knowledge of Building Security and Personal Safety Issues, OIG-CA-03-015, 3/17/03
OCC, General Management: Office of the Comptroller of the Currency Respondents Feel Safer When They Know Security and Safety Procedures, OIG-CA-03-016, 3/17/03
OTS, General Management: Most Office of Thrift Supervision Employee Feelings to Knowing Building and Security Procedures, OIG-CA-03-017, 3/17/03
FMS, General Management: Washington, D.C. Area Financial Management Service Respondents Feel Safe at their Workplace, OIG-CA-03-018, 3/18/03
Mint, General Management: Although Greater Washington, D.C. Area Mint Respondents Indicated Feeling Safe at Their Workplace, They Lack Knowledge of Security Procedures, OIG-CA-03-019, 3/18/03
BEP, Information Technology: Security Vulnerabilities Pose Risks to the Bureau of Engraving and Printing's Network and Systems **(LOU)**, OIG-03-070, 3/27/03

Overseeing the Management of the Nation's Revenue and the Public Debt
Customs, Revenue Collection: Enhanced Controls Could Prevent Improper Payment of Customs Drawback Claims, OIG-03-026, 12/2/02
Customs, Customs ACE Management: Improved Management of Reengineering Needed, OIG-03-058, 2/13/03

Recent Reports

Assessing Law Enforcement Programs

FinCEN, Money Laundering/Bank Secrecy Act: FinCEN Needs to Strengthen Its Efforts To Deter and Detect Money Laundering in Casinos, OIG-03-001, 10/1/02
Customs, Protecting the Public: Customs Faces Staffing Challenges Along the Northern Border, OIG-CA-03-002, 10/31/02
Secret Service, Protecting the Public: U.S. Secret Service's Control Over Seized Property Needs Improvement, OIG-03-013, 11/5/02
ATF, Protecting the Public: The Bureau of Alcohol, Tobacco and Firearms' Youth Crime Gun Interdiction Initiative Program Implementation, OIG-03-019, 11/20/02
Customs, Trade And Passenger Processing: Customs' IPR Enforcement Strategy and Management Controls Over the IPR Module Need to Be Strengthened, OIG-03-027, 12/3/02
FinCEN, FinCEN: Reliability of Suspicious Activity Reports, OIG-03-035, 12/18/03
FLETC, Training Operations: FLETC's Actions to Reduce a Reported Material Weakness Associated With Operation of Its Outdoor Dirt Berm Ranges, OIG-03-036, 12/19/02
Customs, Protecting the Public: Security, Inspection, and Targeting of Vessel Containers at Ports of Los Angeles and Long Beach Can Be Improved **(LOU)**, OIG-03-041, 12/26/02
Customs, Trade Processing: The HAZMAT Program at the Port of Houston Needs to be Strengthened **(LOU)**, OIG-03-049, 1/22/03
Customs, Passenger Processing: Changes to the Advance Passenger Information System Have Been Made But Its Value as an Enforcement Tool is Dependent on Factors Outside Customs Control **(LOU)**, OIG-03-059, 2/12/03
Customs, Protecting the Public: Targeting, Inspection, and Security of Vessel Containers at the Port of Philadelphia Can be Improved **(LOU)**, OIG-03-060, 2/21/03
Customs, Protecting the Pubic: Customs Policies, Procedures, and Training for Racial and Ethnic Profiling – A Comparative Review, OIG-CA-03-008, 2/24/03
Secret Service, Protecting the Public: Secret Service Policies, Procedures, and Training for Racial and Ethnic Profiling – A Comparative Review, OIG-CA-03-009, 2/24/03
Multi-Bureau, Protecting the Public: Law Enforcement Bureaus Claim Information Sharing Within Treasury to be Adequate, OIG-CA-03-012, 2/28/03
Customs, Bank Secrecy Act: Implementation of the Report of International Transportation of Currency or Monetary Instruments (CMIR), OIG-03-062, 3/4/03
Customs, Protecting the Public: Security, Inspection and Targeting of Vessel Containers at the Port of Charleston Can be Improved **(LOU)**, OIG-03-063, 2/28/03
Customs, Trade Processing: The National HAZMAT Program Needs to be Strengthened **(LOU)**, OIG-03-065, 3/17/03
Customs, Protecting the Pubic: Security, Inspection, and Targeting of Vessel Containers at the Ports of New York and Newark Can Be Improved **(LOU)**, OIG-03-066, 3/20/03
ATF, Treasury General Management: Actions Needed to Improve Operations at The Bureau of Alcohol, Tobacco, and Firearms' Philadelphia Field Division **(LOU)**, OIG-03-067, 3/24/03
Customs, Protecting the Public: Customs' Utilization of Trace Detection Equipment Needs to be Improved **(LOU)**, OIG-03-068, 3/24/03
Multi-Bureau, Export Enforcement: Numerous Factors Impaired Treasury's Ability to Effective Enforce Export Controls **(LOU)**, OIG-03-069, 3/25/03
Customs, Protecting the Public: United States Customs Service Enforcement Operations for Inbound Railcars at Port Huron, MI **(LOU)**, OIG-03-071, 3/26/03
Customs, Protecting the Public: Customs Is Not Adequately Monitoring Transportation of International Mail and Needs to Enhance Examinations to Identify Revenue and Effectively Combat Terrorism **(LOU)**, OIG-03-072, 3/27/03, **$1,482,000,000 R**

Recent Reports

Customs, Protecting the Public: Customs Needs a Strategic Plan for Deploying Radiation Detection Equipment **(LOU),** OIG-03-073, 3/27/03
Customs, Protecting the Public: Security, Inspection and Targeting of Vessel Containers At U.S. Seaports Can Be Improved **(LOU)**, OIG-03-074, 3/28/03

Working to Maintain Confidence in the Nation's Banking System
OCC, Material Loss Review of NextBank, NA, OIG-03-024, 11/26/02
OCC, Material Loss Review of Hamilton Bank, NA, OIG-03-032, 12/17/02

Supervised Contract Audits
BEP, Subcontract Proposal Submitted Under Solicitation BEP-02-04 For Security Thread, OIG-03-003, 10/9/02, **$7,409,640 S**
ATF, Direct and Indirect Costs and Rates for Fiscal Year Ended December 18, 1998, OIG-03-006, 10/16/02
Mint, Agreed-Upon Procedures to Final Incurred Costs Plus Fee for United States Mint Contracts, OIG-03-008, 10/23/02
ATF, Costs Incurred for Contractor's Fiscal Year Ending December 31, 1997, OIG-03-010, 11/4/02
Customs, Costs Incurred for Contractor's Fiscal Year Ending December 31, 1997, OIG-03-011, 11/4/02
Customs, Costs Incurred for Contractor's Fiscal Year Ending December 31, 1997, OIG-03-012, 11/4/02, **$110,800 Q**
Customs, Cost Incurred for Fiscal Year 1998, OIG-03-056, 2/5/03, **$31,570 Q**

References to the Inspector General Act and Acronyms

References to the Inspector General Act of 1978, as amended		
Reference	Requirement	Page
Section 4(a)(2)	Review of legislation and regulations	2
Section 5(a)(1)	Significant problems, abuses, and deficiencies	5-20
Section 5(a)(2)	Recommendations with respect to significant problems, abuses, and deficiencies	5-20
Section 5(a)(3)	Significant unimplemented recommendations described in previous semi-annual reports	42-43
Section 5(a)(4)	Matters referred to prosecutive authorities	38
Section 5(a)(5)	Summary of instances where information was refused	38
Section 5(a)(6)	List of audit reports	44-48
Section 5(a)(7)	Summary of significant reports	4-37
Section 5(a)(8)	Audit Reports with Questioned Costs	39
Section 5(a)(9)	Recommendations that funds be put to better use	39-40
Section 5(a)(10)	Summary of audit reports issued before the beginning of the reporting period for which no management decision has been made (Reports with Pending Management Decisions)	41
Section 5(a)(11)	Significant revised management decisions made during the reporting period	38
Section 5(a)(12)	Management decisions with which the Inspector General is in disagreement	47
Section 5(a)(13)	Instances of unresolved FFMIA non-compliance	7

Acronyms

ACE	Automated Commercial Environment
AES	Automated Export System
AIGA	Assistant Inspector General for Audit
AIGI	Assistant Inspector General for Investigations
APIS	Advance Passenger Information System
ATF	Bureau of Alcohol, Tobacco and Firearms
BEP	Bureau of Engraving and Printing
BPD	Bureau of the Public Debt
BSA	Bank Secrecy Act
CDFI Fund	Community Development Financial Institutions Fund
CFO	Chief Financial Officer
CIO	Chief Information Officer
CMIR	Currency or Monetary Instruments
CMO	Customs Modernization Office
COOP	Continuity of Operations Planning
CPS	Certificate Policy Statement
Customs	U.S. Customs Service
DC	District of Columbia
DCAA	Defense Contract Audit Agency
DD/SAC	Division Director/Special Agent-in-Charge
DHS	Department of Homeland Security
DO	Departmental Offices
EDP	Electronic Data Processing

References to the Inspector General Act and Acronyms

EPACT	Energy Policy Act
ESS	Employee Suitability System
FDIA	Federal Deposit Insurance Act
FDIC	Federal Deposit Insurance Corporation
FFB	Federal Financing Bank
FFMIA	Federal Financial Management Improvement Act of 1996
FinCEN	Financial Crimes Enforcement Network
FLETC	Federal Law Enforcement Training Center
FMS	Financial Management Service
FTE	Full-time Equivalent
FY	Fiscal Year
GCB	Gaming Control Board
GMRA	Government Management Reform Act
HSA	Homeland Security Act
ICIG	Intelligence Community Inspectors General
IDMS	Integrated Document Management System
IMB	International Mail Branches
INS	Immigration and Naturalization Service
IPA	Independent Public Accountant
IPO	Initial Public Offering
IPR	Intellectual Property Rights
IRS	Internal Revenue Service
IT	Information Technology
Justice	Department of Justice
Mint	U.S. Mint
NECPA	National Energy Conservation Policy Act
NCIC	National Crime Information Center
NIC	National Intelligence Community
OA	Office of Audit
OC	Office of Counsel
OCC	Office of the Comptroller of the Currency
OFAC	Office of Foreign Asset Control
OI	Office of Investigations
OIG	Office of Inspector General
OIS	Office of Intelligence Support
OM	Office of Management
OMB	Office of Management and Budget
OSHE	Office of Safety, Health and Environment
OTS	Office of Thrift Supervision
PKI	Public Key Infrastructure
SAR	Suspicious Activity Report
SARC	Suspicious Activity Report by Casino
Secret Service	U.S. Secret Service
SED	Shipper's Export Declaration

TCS	Treasury Communications System
TECS	Treasury Enforcement Communications System
TFF	Treasury Forfeiture Fund
TIGTA	Treasury Inspector General for Tax Administration
TTB	Alcohol and Tobacco Tax and Trade Bureau
USPS	United States Postal Service
YCGII	Youth Crime Gun Interdiction Initiative

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 Counsel
740 15th Street, N.W., Suite 110
Washington, D.C. 20220
Phone: (202) 927-0650; Fax (202) 927-5418

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

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

Western Regional 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

Treasury OIG Web Page

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