DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

October 16, 2006

MEMORANDUM FOR SECRETARY PAULSON

FROM: Harold Damelin
Inspector General

SUBJECT: Management and Performance Challenges Facing the Department of the Treasury (OIG-CA-07-002)

The Reports Consolidation Act of 2000 requires that we provide you with our perspective on the most serious management and performance challenges facing the Department of the Treasury, for inclusion in the Department's annual performance and accountability report.

Last year we identified five challenges that we believe seriously impeded the Department's ability to conduct its program responsibilities and ensure the integrity of its operations. These challenges are: (1) Corporate Management, (2) Management of Capital Investments, (3) Information Security, (4) Linking Resources to Results, and (5) Anti-Money Laundering and Terrorist Financing/Bank Secrecy Act Enforcement. While some progress on each of these five challenges has been made, they continue to represent significant risks to the Department. Listed below is a detailed discussion of each challenge.

Challenge 1 – Corporate Management

This is an overarching management challenge. Treasury needs to provide effective corporate leadership in order to resolve serious bureau and program office deficiencies that adversely impact the performance of Treasury as a whole. In particular, Treasury needs to assert strong leadership and supervision over the Internal Revenue Service (IRS) to resolve the longstanding material weaknesses and system deficiencies that hamper the timely and reliable information necessary to effectively manage IRS operations. In addition, while progress has been made, the Department has not fully implemented a corporate-level control structure to ensure that capital investments are properly managed, information about government operations and citizens is adequately secured, and financial resources used by Treasury can be linked to its operational results. These matters are discussed in more detail in the following challenges.

The increasing emphasis on agency-wide accountability envisioned in the management reform legislation of the past decade and the President's Management Agenda, has underscored the need for effective corporate management at Treasury. With nine bureaus and many program offices, Treasury is a highly decentralized organization. As such, Treasury management should ensure consistency, cohesiveness, and economy among all bureaus and program offices in achieving Treasury's goals and objectives. Inherent in this is the need for clear lines of accountability between corporate, bureau, and program office management; enterprise solutions for core business activities; consistent application of accounting principles; and effective oversight of capital investments and information security.

This past year, the Department's senior leadership has asserted more direct and substantive involvement in developing and implementing Treasury-wide polices and initiatives across a number of fronts. For example, Treasury established, for the first time, a substantially complete systems inventory. This is a critical step to ensuring security over its information technology assets. Also, the Deputy Secretary recently issued a memorandum requiring that internal control programs (programs to ensure accountability and promote effective management and stewardship) be included in all fiscal year 2007 senior leadership performance plans. In the future, this type of direct involvement by senior leadership needs to be maintained so that progress continues.

Challenge 2 – Management of Capital Investments

Treasury needs to better manage large acquisitions of mission-critical systems and other capital investments. In the past, we discussed serious problems related to the Treasury Communications Enterprise (TCE) procurement, Treasury's HR Connect system, and the Treasury and Annex Repair and Restoration (TBARR) project.

This year, we note continuing issues with TCE and new problems have been brought to light with BSA Direct, and the web-based Electronic Fraud Detection System (Web EFDS). Specifically, we found that the TCE procurement, estimated to cost $1 billion over its useful life, was poorly planned, executed, and documented. For example, Treasury's consideration of General Services Administration contract vehicles, both at the outset and following a successful TCE bid protest, was incomplete, and the TCE business case documentation was deficient. Treasury amended and reopened the TCE solicitation in October 2005, but has yet to award the TCE contract. In July 2006, after nearly 2 years in development and $15 million spent, the Financial Crimes Enforcement Network (FinCEN) terminated its contract for the storage and retrieval component of BSA Direct after significant concerns were raised about schedule delays and project management. IRS had similar problems with Web EFDS, a system costing more than $20 million intended to prevent fraudulent refunds. In April 2006, after a significant delay, IRS stopped all development activities for Web EFDS. IRS also was unable to use EFDS to prevent fraudulent refunds during processing year 2006. The Treasury Inspector General for Tax Administration reported that without Web EFDS, more than $300 million in fraudulent refunds may have been allowed.

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

Challenge 3 – Information Security

Despite some notable accomplishments, the Department needs to improve its information security program and practices to achieve compliance with the Federal Information Security Management Act of 2002 (FISMA) and Office of Management and Budget (OMB) requirements. In the past, we reported that Treasury's systems inventory was not accurate, complete, or consistently reported. During the past year, the Department overcame this weakness in its security program by providing direction to the bureaus in developing a Department-wide inventory of information systems. Although the Department still needs to

implement additional actions to further improve the system inventory, we believe the inventory is substantially complete and generally conforms to applicable requirements.

Nevertheless, our 2006 FISMA evaluation disclosed deficiencies that, in the aggregate, constitute substantial noncompliance with FISMA. Specifically, we noted that improvements are needed in the areas of: certification and accreditation, security awareness, training employees with significant security responsibilities, tracking corrective actions, identifying and documenting system interfaces, security self-assessments, configuration management, and incident response. As a result of the improved inventory, Treasury identified that it has national security systems that are not part of its intelligence program. For the first time, we evaluated the information security program and practices as it relates to these non-intelligence national security systems. We noted that significant improvements are also needed in this area.

During 2006, OMB issued Memorandum 06-16, *Protection of Sensitive Agency Information* (M-06-16), requiring agencies to perform specific actions to protect certain personally identifiable information. Our evaluation of Treasury's compliance with M-06-16 disclosed that Treasury still faces significant challenges to meet these requirements. Specifically, we noted that the Department needs to ensure that security controls pertaining to personally identifiable information are addressed Treasury-wide in the following areas: assessing risk, reviewing and revising policies, transporting, offsite storage, and remote access. In a July 2006 memorandum to Treasury bureaus, the Department provided implementation guidance and required bureaus to identify their specific actions taken and planned, including dates, to address weaknesses in security controls pertaining to personally identifiable information.

Challenge 4 – Linking Resources to Results

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

The Government Accountability Office (GAO) reported in December 2005 that Treasury delegated to its bureaus responsibility to implement MCA systems and processes to meet federal standards. Although Treasury retained oversight responsibility to ensure consistent implementation of MCA department-wide, Treasury officials had no specific procedures in place to ensure that consistent, periodic department-level oversight was conducted, and they promoted MCA and monitored MCA implementation on an informal and sporadic basis. This contributed to widely disparate implementation and use of MCA among Treasury's program offices and bureaus. GAO also found that controls to ensure the reliability of MCA data needed improvement in two of the three Treasury bureaus it reviewed.

Since GAO's review, the Department has developed a high-level MCA implementation plan. This plan focuses on (1) clarifying and reaffirming the Department's MCA policy for all bureaus; (2) identifying MCA needs across the Department; (3) ensuring MCA needs are linked to the Department's strategic plan, budget, and performance measures; (4) identifying gaps

between Department and bureau needs and existing MCA capabilities; and (5) developing plans to eliminate these gaps. However, none of the specific action items in the plan have been completed and target dates for certain actions have been missed.

Challenge 5 – Anti-Money Laundering and Terrorist Financing/Bank Secrecy Act Enforcement

Treasury faces unique challenges in carrying out its responsibilities under the Bank Secrecy Act (BSA) and USA Patriot Act to prevent and detect money laundering and terrorist financing. To effectively prevent and detect financial crimes and terrorist financing it is necessary to have: (1) strong control environments at financial institutions that ensure that business is conducted with reputable parties, and large currency transactions and suspicious activities are properly and timely reported to Treasury, (2) strong federal and state regulatory agencies that examine and enforce BSA and USA Patriot Act requirements at financial institutions, and (3) strong analytical capacity to identify and refer to law enforcement leads provided through reports filed by financial institutions.

While FinCEN is the Treasury bureau responsible for administering BSA, it relies on other Treasury and non-Treasury agencies to enforce compliance with the Act's requirements. The Office of Foreign Assets Control (OFAC), the Treasury office responsible for administering U.S. foreign sanction programs, also relies on other Treasury and non-Treasury agencies to ensure compliance with OFAC requirements. Past audits and Congressional hearings, however, have surfaced serious regulatory gaps in the detection of and/or timely enforcement action against financial institutions for BSA and related violations. For example, a recent audit found that the Office of the Comptroller of the Currency (OCC) took a questionable (non-public) enforcement action when it found serious recurring BSA program deficiencies at the nation's fifth largest bank. Another recent audit found that FinCEN was slow in developing possible new leads for law enforcement through analysis of BSA data, devoting most of its analytical work to processing routine data requests. Another recent audit found that OCC and Office of Thrift Supervision (OTS) examinations of financial institutions for OFAC compliance were not documented well enough to determine whether the examined institutions were in compliance.

In an attempt to improve compliance and address some of these gaps, Treasury created the Office of Terrorism and Financial Intelligence (TFI) through which FinCEN and OFAC now report. In addition, FinCEN, beginning in 2004, (1) created a compliance office to improve BSA oversight and coordination with financial institution regulators; and (2) entered into memoranda of understanding (MOUs) with the federal banking regulators, IRS, and most states to enhance communication and coordination. Furthermore, OCC and OTS took immediate steps to improve their respective documentation of OFAC examinations. Additionally, OFAC also executed MOUs with the federal banking regulators that provides for increased information sharing. While similar to the MOUs between FinCEN and the regulators, legislative impairments may ultimately limit the information shared with OFAC. For this reason and others, the effectiveness of these actions to address regulatory gaps and ultimately improve compliance is yet to be determined.

Given the criticality of this management challenge to the Department's mission, we will continue to devote a significant portion of our audit resources on TFI, FinCEN, OFAC, OCC, and OTS programs and operations. For example, we are planning comprehensive reviews of the effectiveness of (1) FinCEN's Office of Compliance, and (2) the MOUs that have been established.

We would be pleased to discuss our views on these management and performance challenges in more detail.

cc: Robert M. Kimmitt
Deputy Secretary

Sandra L. Pack
Assistant Secretary for Management and Chief Financial Officer