DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

October 16, 2017

INFORMATION MEMORANDUM FOR SECRETARY MNUCHIN

FROM: Eric M. Thorson /s/
Inspector General

SUBJECT: Management and Performance Challenges Facing the Department of the Treasury (OIG-CA-18-002)

In accordance with the Reports Consolidation Act of 2000, we are providing you with our perspective on the most serious management and performance challenges facing the Department of the Treasury (hereinafter Treasury or the Department).

We are reporting four challenges of which one is new and three are updated from last year.

- Operating in an Uncertain Environment (New Challenge)
- Cyber Threats
- Anti-Money Laundering and Terrorist Financing/Bank Secrecy Act Enforcement
- Efforts to Promote Spending Transparency and to Prevent and Detect Improper Payments

This year, we removed "Management of Treasury's Authorities Intended to Support and Improve the Economy" that was reported as a challenge in the prior year's memorandum. We had reported this as a challenge for the past several years as Treasury has had to administer large dollar initiatives related to authorities created to address the financial crisis as enacted under the Housing and Economic Recovery Act of 2008, the American Recovery and Reinvestment Act of 2009, the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank), and the Small Business Jobs Act of 2010. In addition, Treasury was given authority under the Resources and Ecosystems Sustainability, Tourist Opportunities, and Revived Economies of the Gulf Coast States Act of 2012 to address the specific economic and environmental restoration of the Gulf Coast region. We no longer consider Treasury's management of these authorities as a continuing challenge since the offices and programs established to implement and administer the requirements have been in place for a number of years and several programs are reaching maturity.

In addition to the above challenges, we continue to report our elevated concerns about two matters: currency and coin production and documenting key activities and decisions.

2018 Management and Performance Challenges

Challenge 1: Operating in an Uncertain Environment

In assessing the Department's most serious challenges, we remain mindful of external factors and future uncertainties that affect its operations. Most notable are the proposed budget cuts and new requirements imposed by Executive Order (E. O.) 13781, *Comprehensive Plan for Reorganizing the Executive Branch* (March 13, 2017). In its implementation of E. O. 13781, the Office of Management and Budget (OMB) required agencies to submit Agency Reform Plans, which include long-term workforce plans and that are in alignment with their strategic plans, to OMB concurrently with their fiscal year 2019 budget requests. These plans are to include proposals in four categories: eliminate activities; restructure or merge; improve organizational efficiency and effectiveness; and workforce management. After consideration of all Agency Reform Plans, OMB intends to work with agencies in developing crosscutting reform proposals that involve multiple agencies, which could include merging agencies, components, programs, or activities that have similar missions. These proposals, along with the agency plans and public input, will be used by OMB in developing its comprehensive Government–wide Reform Plan to reorganize the Executive Branch.[1]

Needless to say, OMB's Government–wide Reform Plan may significantly impact the administration of the Department's programs and operations. With looming uncertainties as to the impact of the plan, the Department must plan for the potential long-term restructuring of certain functions or offices/bureaus and/or budget cuts. This may require the Department to take immediate actions to achieve near-term cost savings while focusing its limited resources on programs that are in the highest need to citizens and/or where there is a unique Federal role. That said, it is also essential that these reforms be managed and communicated effectively such that performance and accountability can be improved and missions can still be met throughout the Department.

Another related uncertainty facing the Department involves the repeated cycle of budget and debt ceiling stopgaps. As I reported in my last memorandum to you, Congress has yet to resolve unfinished business when it comes to the Nation's debt, and the long-term sustainability of the large programs. Although legislation was passed to temporarily extend the debt limit until December 8, 2017, no long-term solution has been found.

Tackling these more critical matters at hand could be more challenging as several Presidentially-appointed, Senate-confirmed leadership positions within Treasury remain vacant since January 2017. Further complicating this, the Federal Vacancies Reform Act of 1998 requires executive branch agencies to report to Congress and the Government Accountability Office (GAO) information on the temporary filling of executive agencies' vacant Presidentially-appointed, Senate-confirmed positions. The Department will soon, if not already, reach the 210 day provisions for some temporary acting positions.

---

[1] OMB, M-17-22, *Comprehensive Plan for Reforming the Federal Government and Reducing the Federal Civilian Workforce* (April 12, 2017)

Challenge 2: Cyber Threats

Cybersecurity is a long-standing and serious challenge facing the Nation today. A reliable critical infrastructure, including information systems and networks, is vital to our national security and economic stability. Cyber threats are a persistent concern as Treasury's information systems are critical to the core functions of government and the Nation's financial infrastructure. As cyber threats continue to evolve and become more sophisticated and subtle, they pose an ongoing challenge for Treasury to fortify and safeguard its internal systems and operations and the financial sector it oversees. Effective public-private coordination continues to be required to address the cyber threat against the Nation's critical infrastructure. In this regard, Treasury is looked upon to provide effective leadership to financial institutions in particular, and the financial sector in general, to strengthen awareness and preparedness against cyber threats.

Attackers frequently exploit vulnerable networks in a string of trusted connections to gain access to government systems. Attempted cyber-attacks against Federal agencies, including Treasury, and financial institutions are increasing in frequency and severity, and continue to evolve at an accelerated rate. Such attacks include distributed denial of service attacks, phishing or whaling attacks, fraudulent wire payments, malicious spam (malspam), and ransomware. Organized hacking groups leverage published and unpublished vulnerabilities and vary their methods to make attacks hard to detect and even harder to prevent. Criminal groups and nation-states are constantly seeking to steal information; commit fraud; and disrupt, degrade, or deny access to information systems. In addition to Treasury's own networks and systems, management must be cognizant of, and mitigate, the risks posed by attacks made against other agencies and Treasury contractors and subcontractors. Treasury frequently enters into interconnection agreements with other Federal, State, and local agencies, and service providers, to conduct its business. Treasury management must exercise due care when authorizing such internetwork connections and verify that third parties comply with Federal policies and standards. Management is also challenged with ensuring that critical data and information maintained by cloud service providers are properly protected.

Ensuring the government has a sufficient number of cybersecurity professionals is an ongoing challenge that was reported by GAO not long ago.[2] Similarly, the results of OMB's Cybersecurity Sprint identified the lack of cybersecurity and information technology talent as a major resource constraint for Federal agencies. The cybersecurity sprint highlighted the need for agencies to improve recruitment, retention, and training of their information technology workforce. In our audits of select Treasury bureaus, we continue to find that causes for many of our findings related to information systems' security measures involved a lack of resources and/or management oversight, which echoed GAO and OMB's observations of agencies' impairments. I would like to note that my office has not been immune from these same difficulties as overseeing Treasury's cyber and information security programs becomes increasingly challenging with our current resources.

[2] GAO, *Actions Needed to Address Challenges* (GAO-16-885T; issued September 19, 2016)

Challenge 3: Anti-Money Laundering and Terrorist Financing/Bank Secrecy Act Enforcement

As previously reported, identifying, disrupting, and dismantling the financial networks that support terrorists, organized transnational crime, weapons of mass destruction proliferators, and other threats to international security continue to be challenging. Treasury's Office of Terrorism and Financial Intelligence (TFI) is dedicated to disrupting the ability of terrorist organizations to fund such activities through intelligence analysis, sanctions, and international private-sector cooperation that identify donors, financiers, and facilitators funding terrorist organizations.

TFI's ability to effectively gather and analyze intelligence information on financial crimes and terrorism requires a stable cadre of staff. Concerns over TFI's ability to meet mission critical objectives are heightened by multiple vacant key positions. Some key leadership positions have been vacant for a number of years, including the Director of the Financial Crimes Enforcement Network (FinCEN), the Assistant Secretary of Intelligence and Analysis, and Deputy Assistant Secretaries. Because of TFI's complementary missions in intelligence gathering and coordination with international and domestic intelligence and law enforcement entities, stability and coordination within TFI is imperative to reduce duplication, enhance information gathering and intelligence analysis, and increase efficiency.

Major challenges for the U.S. and Treasury involve stopping the Islamic State of Iraq and Syria (ISIS), rogue regimes and countries, and other bad actors who want to harm people and properties and disrupt the global financial system. Stopping ISIS depends on a whole-of-government approach to combating terrorism and other illicit financing and requires collaboration and coordination within Treasury and with other Federal agencies. Coordination and collaboration are key to successfully tracking and disrupting terrorist and other criminal networks and requires TFI regularly work with interagency partners to leverage diplomatic engagement, regulatory and law enforcement, and intelligence collection and analysis tools. The effort to disrupt ISIS requires an effective and efficient working relationship within TFI, including FinCEN and the Office of Foreign Assets Control (OFAC).

OFAC's administration of U.S. sanction programs is constantly evolving. Most notable were the significant changes to the Iran and Cuba sanction programs. Trade sanctions with Cuba has eased some since 2014 resulting from a regime change and improved relations. The U.S. eased nuclear-related sanctions with Iran, but continued imposing sanctions made pursuant to existing laws and related to Iran's human rights policies, support for terrorism, interference in specified countries in the region, and missile and advanced conventional weapons programs. The sanctions continue to bar U.S. individuals and entities from most forms of investment in or trade with Iran. In other areas, the U.S. has increased sanctions against the North Korea for missiles testing and Russia for its assertiveness towards other countries, including the U.S.

Enhancing the transparency of the financial system is one of the cornerstones of the effort to disrupt the ability of terrorist organizations. FinCEN faces continuing challenges to enhance financial transparency and strengthen efforts to combat financial crime and collect, analyze, and report data on national and international threats. FinCEN has focused on enhancing enforcement efforts through compliance with the Bank Secrecy Act (BSA) in partnership with Federal banking regulators and law enforcement. FinCEN's key initiatives to strengthen financial transparency include, among other things, issuing rules and regulations such as the Customer

Due Diligence rule that required financial institutions to identify beneficial ownership of financial accounts of legal entity customers. FinCEN is also challenged with providing clarifying guidance to financial institutions that are reluctant to do business with State-legalized marijuana dispensaries. While these dispensaries remain illegal under Federal law, increasingly, states have passed laws allowing businesses to dispense marijuana. Other areas of concern for FinCEN include the increasing use of (1) mobile banking, internet banking, internet gaming, and peer-to-peer transactions; and (2) money service businesses, including virtual currency administrators and exchanges.[3] FinCEN and other regulatory agencies will need to ensure that providers of these services who are covered by BSA understand their obligations to report information to FinCEN.

Given the criticality of Treasury's mission to combat terrorist financing and money laundering, we continue to consider anti-money laundering and combating terrorist financing programs and operations as inherently high-risk.

Challenge 4: Efforts to Promote Spending Transparency and to Prevent and Detect Improper Payments

Spending Transparency

Treasury continues to make progress in its Government-wide and Department-wide implementation of the Digital Accountability and Transparency Act of 2014 (DATA Act). The DATA Act requires the Federal Government to provide consistent, reliable, and useful online data about how it spends taxpayer dollars. To fulfill its purposes, the DATA Act imposed several mandates on the Director of OMB, the Secretary of the Treasury, the Inspector General of each Federal agency, and the Comptroller General of the United States. Several of these mandates have already been successfully met. As required within one year after enactment, on May 8, 2015, OMB and Treasury standardized 57 Government-wide financial data elements for Federal funds made available to or expended by Federal agencies and entities receiving Federal funds.

On May 9, 2017, Treasury, in consultation with OMB, met its second mandate to ensure that financial data was posted, in accordance with the financial data standards established by Treasury and OMB, and displayed on USAspending.gov[4] within two years after enactment of the DATA Act.

While there have been reported successes to date, OMB and Treasury must still ensure the data standards established are applied to the data made available on USAspending.gov by May 2018. The Department continues to make progress in its efforts to comply with the DATA Act by executing its comprehensive implementation plan that conforms to the Government-wide technical and informational guidance issued by OMB and Treasury. Given the broad

---

[3] Bitcoins are an example of a virtual currency. These consist of a series of numbers created automatically on a set schedule and traded anonymously between digital addresses or "wallets." Certain exchange firms buy or sell Bitcoins for legal tender at a rate that fluctuates with the market. Congress and regulators continue their efforts to determine the legality, legitimacy, and regulatory framework for virtual currencies such as Bitcoins.

[4] In May 2017, Treasury launched a new version of USAspending.gov, currently referred to as Beta.USAspending.gov, which is being run parallel to USAspending.gov to minimize disruptions to users' access and add system enhancements. Treasury intends to retire the legacy USAspending.gov in fall 2017.

implications and critical roles assigned to Treasury by the DATA Act, we consider this an ongoing high risk implementation project and management challenge.

It should be noted that we have initiated a series of audits of Treasury's efforts to meet its responsibilities under the DATA Act. As of this writing, we are performing two DATA Act audits focusing on Treasury's (1) Government-wide implementation efforts, and (2) Department-wide implementation efforts.

Detect Improper Payments

In light of the continuing problem with improper payments (estimated at $144 billion, or 4.67 percent of all program outlays, for fiscal year 2016), the Federal Government has intensified efforts to reduce improper payments in major Federal programs. The Do Not Pay Initiative and the Treasury Bureau of the Fiscal Service's (Fiscal Service) Do Not Pay Business Center are chief components of efforts designed to prevent and detect improper payments to individuals and entities.

The Do Not Pay Business Center provides two services to agencies: the Do Not Pay Portal and the Do Not Pay Data Analytics Service. The Do Not Pay Portal is intended to provide users with a single entry point to search data sources such as the Social Security Administration's (SSA) publicly available Death Master File, the Department of Health and Human Service Office of Inspector General's List of Excluded Individuals/Entities, the General Services Administration's System for Award Management, and Treasury's Debt Check Database. However, as we reported in November 2014, the effectiveness of the Do Not Pay Business Center as a tool to prevent and detect improper payments is hindered because the center does not have access to, among other things, SSA's full death data.[5] In October 2016, GAO reported that restrictions on the center's access to SSA's full death data remained in place.[6]

The Do Not Pay Data Analytics Service supports agencies' efforts to identify and prevent improper payments by identifying trends and patterns in agency payment and other information that may be indicative of improper payments. The results of these analyses are provided to agencies at no cost for further study so they can prevent future improper payments. We have on-going audit work assessing the services provided to agencies by the Do Not Pay Data Analytics Service.

With its potential to reduce improper payments, the Do Not Pay Business Center is a major and important undertaking by Fiscal Service and Treasury. As part of our ongoing audit work in this area, we will continue to monitor the steps taken by Fiscal Service to improve the effectiveness of the Do Not Pay Business Center. We are also planning to review the Do Not Pay Program's data analytic capabilities during the coming fiscal year.

---

[5] OIG, *Fiscal Service Successfully Established the Do Not Pay Business Center But Challenges Remain* (OIG-15-006; November 6, 2014)

[6] GAO, *Improper Payments, Strategy and Additional Actions Needed to Help Ensure Agencies Use the Do Not Pay Working System as Intended* (GAO-17-15; issued October 14, 2016)

Other Matters of Concern

Although we are not reporting these as management and performance challenges, we are highlighting two areas of concern that are repeated from last year's letter: (1) currency and coin production, and (2) documenting key activities and decisions.

Currency and Coin Production

Challenges continue to exist with coin and currency production at the Bureau of Engraving and Printing (BEP) and the United States Mint (Mint). In the case of the Mint, the costs of producing penny and nickel coins were double their face value because of rising metal prices resulting in higher production costs. The Mint continues to review U.S. currency to include the production and use of coins, the use of alternative metals, and the suitability of Mint facilities for production. The Mint must also ensure strong internal controls are in place to safeguard the integrity and protect U.S. coinage. This is done by preventing the acceptance of illegitimate coinage under its redemption program which is planned to be reinstated in 2017, as well as maintaining proper physical security at all Mint facilities. For BEP, it is imperative that effective project management practices are applied to thwart counterfeiters and identify and implement counterfeit deterrence features in a timely manner to safeguard U.S. currency from this significant threat.

In addition, BEP and the Mint need to consider the effect of alternative payment methods and other technological advances (such as stored value cards, the Internet, smartphones, and virtual currencies) as well as consumer demand on their respective business models, practices, future planning and interactions with their customers, and the Federal Reserve Bank.

Documenting Key Activities and Decisions

Over the years, my office repeatedly cites the Department's and bureaus' lapses in maintaining a complete and concurrent record of key activities and decisions. This continues to be identified as a problem as reported in our more recent audits of Fiscal Service's selection of a financial agent in its rebid of the Direct Express® Debit MasterCard,® the Office of the Comptroller of the Currency's supervision of banks' use of independent consultants, and FinCEN's case files supporting its Bank Secrecy Act enforcement actions.

We believe developing and maintaining proper documentation supports transparency and confidence in Treasury's decision making process. Maintaining proper documentation is a fundamental tenet of government accountability and transparency, and is in the best long-term interest of Treasury and its component offices and bureaus if actions are later questioned, as they have been.

We would be pleased to discuss our views on the management and performance challenges and the other matters expressed in this memorandum in more detail.

cc: Kody H. Kinsley
Assistant Secretary for Management