



OFFICE OF  
INSPECTOR GENERAL

DEPARTMENT OF THE TREASURY  
WASHINGTON, D.C. 20220

October 26, 2016

**INFORMATION MEMORANDUM FOR SECRETARY LEW**

**FROM:** Eric M. Thorson /s/  
Inspector General

**SUBJECT:** Management and Performance Challenges Facing the  
Department of the Treasury (OIG-CA-17-003)

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, which are updated from last year.

- Cyber Threats
- Efforts to Promote Spending Transparency and to Prevent and Detect Improper Payments
- Anti-Money Laundering and Terrorist Financing/Bank Secrecy Act Enforcement
- Management of Treasury's Authorities Intended to Support and Improve the Economy

This year, we combined two challenges that were reported separately in the previous year's memorandum. Specifically, we incorporated last year's Challenge, "Gulf Coast Restoration Trust Fund Administration" into the broader Challenge, "Management of Treasury's Authorities Intended to Support and Improve the Economy." We did this because Treasury has implemented many of the requirements under these authorities. However, given the nature and large dollar amounts provided to Treasury to strengthen and restore the economy, ongoing administration will continue for a number of years.

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. We have also added a new area of concern related to new Enterprise Risk Management (ERM) requirements that Treasury must implement beginning in fiscal year 2017.

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 is the upcoming Presidential election and the transition under a new Administration that change brings. With the change in Administration many Presidentially-appointed, Senate-confirmed leadership positions within Treasury will become vacant. As such, tackling some of the more critical matters at hand could be more challenging.

Another 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 Federal budget, the Nation's debt, and the long-term sustainability of the Social Security and Medicare programs. Although legislation was passed to temporarily extend the debt limit until March 15, 2017, no long-term solution has been found.

Other than the upcoming Presidential election and the resulting change in Administration, many of the circumstances the Department is operating under have remained the same as in the prior year. Cyber threats to Treasury operations and the financial sector will continue to be a serious risk for the foreseeable future. Additionally, Treasury continues to administer programs that are inherently high-risk, such as programs to combat terrorist financing. Throughout the years, Treasury has also been called upon to administer major new programs and initiatives intended to support and improve the country's economy. In nearly every case, the Department has had to start up and administer new programs and operations with thin staffing and very limited, if any, new resources. That situation remains the same and may possibly worsen during a period of transition. Again, we cannot emphasize enough to the Department's stakeholders how critically important it is that Treasury is resourced sufficiently to carry out its authorities and responsibilities to include maintaining a strong control environment.

## **2017 Management and Performance Challenges**

### **Challenge 1: Cyber Threats**

Cybersecurity continues to represent one of the most serious challenges 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.

Attackers frequently exploit vulnerable networks in a string of trusted connections to gain access to government systems. Cyber attacks against Federal agencies are increasing in frequency and severity. The cyber intrusion of the Department of State's networks was used as a route to penetrate computer systems at the White House and gain access to the President's e-mail account. An attack against the Joint Chief of Staff's e-mail forced management to take the system off line, cleanse it, and build in new protections. The recent cyber attacks against the Office of Personnel Management's networks allowed intruders access to personal data on tens of millions of people, including millions with security clearances. According to a recent report issued by the Government Accountability Office (GAO), approximately 1,000 out of 2,500 information security related recommendations made to agencies by GAO were still outstanding. Some of the impairments challenging agencies in implementing their information security programs include an inability to recruit and retain personnel with appropriate skills, not using key security capabilities of their existing systems and devices, use of unsupported or unpatched

software, a lack of in-depth security evaluations, and a lack of consistency in overseeing contractor providing information technology services.<sup>1</sup>

In our recent audits of selected Treasury bureaus, we continue to find that the security measures in place need improvement and many of our findings echo GAO's observations of agencies' impairments, noted above, compounded by competing priorities. 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.

Cyber attacks on financial institutions continue to evolve at an accelerated rate, and include distributed denial of service attacks, phishing attacks, fraudulent wire payments, 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.

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.

## **Challenge 2: Efforts to Promote Spending Transparency and to Prevent and Detect Improper Payments**

### Spending Transparency

The Digital Accountability and Transparency Act of 2014 (DATA Act) requires the Federal Government to provide consistent, reliable, and useful online data about how it spends taxpayer dollars. The stated purpose of the law is to:

- expand the Federal Funding Accountability and Transparency Act of 2006 by disclosing direct Federal agency expenditures and linking Federal contract, loan, and grant spending information to programs of Federal agencies, enabling taxpayers and policy makers to track Federal spending more easily;
- establish Government-wide data standards for financial data and provide consistent, reliable, and searchable Government-wide spending data that is displayed for taxpayers and policy makers on USASpending.gov (or a successor system);
- simplify reporting for entities receiving Federal funds by streamlining reporting requirements and reducing compliance costs while improving transparency;

---

<sup>1</sup> *Actions Needed to Address Challenges* (GAO-16-885T; issued Sept. 19, 2016) <http://www.gao.gov/assets/680/679877.pdf> – Released

- improve the quality of data submitted to USASpending.gov by holding Federal agencies accountable for the completeness and accuracy of the data submitted; and
- apply approaches developed by the Recovery Accountability and Transparency Board to spending across the Federal Government.

Implementing the DATA Act is a complex undertaking requiring a significant level of interagency coordination and cooperation to develop, establish, and apply new financial data standards and to develop new data handling methodologies within a short timeframe. One of the first accomplishments for the Treasury Secretary and the Director of the Office of Management and Budget (OMB) was to establish Government-wide financial data standards for reporting spending by Federal agencies and entities receiving Federal funds by the May 2015 statutory deadline.

After a number of delays, Treasury released its DATA Act information model schema (DAIMS) on April 29, 2016 and the production-ready broker on September 30, 2016. The DAIMS prescribes relationships between data elements as well as format and data reporting validation requirements for transmitting these elements between agencies for publication on USASpending.gov. The production-ready broker collects, maps, transforms, validates, and submits agency data into a format consistent with DAIMS. However, the delays in releasing DAIMS and the production-ready broker, have hindered agencies' ability to determine the full scope of their implementation effort required.

Other key mandates under the act require Treasury and OMB to:

- by May 2017, ensure this financial data is accurately posted and displayed on USASpending.gov, or a successor system; and
- by May 2018, ensure the data standards established are applied to the data made available on the website.

Inspectors General of each Federal agency are required by the act to perform three biennial reviews of a statistically valid sample of spending data submitted by its agency and the implementation of data standards by the agency. Agency Inspectors General must submit to Congress (and make publicly available) a report assessing the completeness, timeliness, quality, and accuracy of the data sampled, as well as the implementation and use of data standards by the Federal agency. As prescribed in the act, the first reports are due November 2016, with two others to follow in November 2018 and November 2020. However, the Inspectors General community identified an anomaly with the timing of these reviews in that the first required report on data submitted is due prior to the date that agencies are required to submit data in accordance with the Act. Therefore, the Treasury Office of Inspector General and the Federal Audit Executive Council DATA Act working group reached out to stakeholders in Congress and crafted a strategy to deal with this anomaly. The strategy was to extend the first required Inspectors General reports from November 2016 to November 2017, and to encourage the Inspectors General to perform "readiness reviews" of their respective agencies before the agency reporting date (and by November 2016, if possible). A letter documenting this strategy was signed by the CIGIE Chairman and sent to Congress on December 22, 2015.

Given the broad Government-wide 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 three DATA Act audits focusing on Treasury's (1) Government-wide implementation efforts, (2) Department-wide implementation efforts, and (3) Bureau of the Fiscal Service's Administrative Resource Center's efforts to report financial spending information on behalf of its customer agencies.

### Detect Improper Payments

In light of the continuing problem with improper payments (estimated at \$136.7 billion, or 4.8 percent of all program outlays, for fiscal year 2015), 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.<sup>2</sup>

With its potential to reduce improper payments, the Do Not Pay Program 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.

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

As we reported in the past, preventing criminals and terrorists from using our financial networks to sustain their operations and/or launch attacks against the U.S. continues to be a challenge. Treasury's Office of Terrorism and Financial Intelligence (TFI) is dedicated to disrupting the ability of terrorist organizations to fund their operations. TFI brings together intelligence gathering and analysis, economic sanctions, international cooperation, and private-sector cooperation to identify donors, financiers, and facilitators supporting terrorist organizations, and disrupt their ability to fund such organizations. Enhancing the transparency of the financial system is one of the cornerstones of this effort.

Treasury carries out its responsibilities to enhance financial transparency through the Bank Secrecy Act (BSA). The Financial Crimes Enforcement Network (FinCEN) is the Treasury

---

<sup>2</sup> OIG, *Fiscal Service Successfully Established the Do Not Pay Business Center But Challenges Remain* (OIG-15-006; Nov. 6, 2014)

bureau responsible for administering BSA, while Treasury's Office of Foreign Assets Control (OFAC) administers U.S. sanction programs.

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 is heightened by multiple key positions left vacant. Some key leadership positions have been vacant for months and even years, including the Under Secretary for TFI and the Directors of FinCEN, OFAC, and the Treasury Executive Office for Asset Forfeiture. A stable workforce is imperative because of TFI's overarching responsibilities in intelligence gathering and coordination with international and public and private sector entities.

With respect to FinCEN, it faces continuing challenges to enhance financial transparency as a way to strengthen efforts to combat financial crime and collect, analyze, and report data on national threats. FinCEN has focused on enhancing its enforcement efforts to promote compliance with the BSA in partnership with Federal banking regulators and law enforcement. It continues to improve its enforcement processes and systems after its 2013 reorganization. Among other things, FinCEN has been working on clarifying and strengthening customer due diligence requirements. This includes requirements for institutions to identify beneficial ownership of their accountholders so that their true identities are not hidden. In May 2016, FinCEN issued the final rule with customer due diligence requirements and a new requirement to identify and verify the identity of beneficial owners of legal entity customers. Also, FinCEN was challenged with providing clarifying guidance to the financial community who may be reluctant to do business with State-legalized marijuana dispensaries. While these dispensaries remain illegal under Federal law, FinCEN's February 2014 guidance for financial institutions clarified reporting obligations with respect to services to marijuana-related businesses consistent with BSA obligations. This guidance includes conducting due diligence on prospective customers. Prepaid cards also present money laundering and terrorist financing risks. In 2011, FinCEN published a notice of proposed rule-making which requires those carrying prepaid cards with values over \$10,000 to declare them at the border (cross-border transactions). In 2015, OMB postponed the issuance of the final rule because it has not completed a budgetary review of the expected final rule.

Other matters of concern on the horizon include the increasing use of (1) mobile devices for banking, internet banking, internet gaming, and peer-to-peer transactions; and (2) virtual currencies.<sup>3</sup> FinCEN and other regulatory agencies will need to make sure that providers of these services who are covered by BSA understand their obligations under the statute. Monitoring the transactions of tomorrow may prove to be increasingly difficult for Treasury. In this regard, in 2013, FinCEN issued guidance on virtual currencies and regulatory responsibilities in order to provide clarity for businesses and individuals engaged in this expanding field of financial activity. FinCEN's rules defined certain businesses or individuals which use convertible virtual currencies or make a business of exchanging, accepting, and transmitting them as Money Service

---

<sup>3</sup> 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.

Businesses (MSBs). MSBs have registration requirements and a range of anti-money laundering, recordkeeping, and reporting responsibilities under FinCEN's regulations.

Given the criticality of this challenge to the Department's mission, and notwithstanding the efforts described above, we continue to consider anti-money laundering and combating terrorist financing programs and operations as inherently high-risk.

#### **Challenge 4: Management of Treasury's Authorities Intended to Support and Improve the Economy**

Congress provided Treasury with broad authorities to address the financial crisis under the Housing and Economic Recovery Act of 2008 (HERA), the American Recovery and Reinvestment Act of 2009 (Recovery Act), and the Small Business Jobs Act of 2010. In response to the call for further financial reform, Congress passed Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank) in 2010. To address the more specific economic and environmental damage caused by the *Deepwater Horizon* oil spill in the Gulf Coast, Treasury was given authority to administer the Gulf Coast Restoration Trust Fund (Trust Fund) established under the Resources and Ecosystems Sustainability, Tourist Opportunities, and Revived Economies of the Gulf Coast States Act of 2012 (RESTORE Act). We also note that Treasury continues to administer programs established under the Troubled Asset Relief Program. That program, however, is not under the jurisdictional oversight of our office.

As we stated last year, to a large extent Treasury's program administration under these acts has matured, but challenges remain in managing Treasury's programs and its outstanding investments as well as ensuring financial reform and economic recovery. Our discussion of this challenge will begin with reforms under Dodd-Frank and then address the others for which Treasury is responsible.

#### Continued Implementation of Dodd-Frank

Among other things, Dodd-Frank established the Financial Stability Oversight Council (FSOC), which you chair as the Treasury Secretary. FSOC accomplished much over the past year. It issued its sixth annual report in June 2016 as required, and rescinded the designation of one nonbank financial company for supervision by the Board of Governors of the Federal Reserve System (FRB). Additionally, FSOC released the results of a study on the effects of size and complexity of financial institutions on capital market efficiency and economic growth. FSOC continues its analysis of potential financial stability risks that may arise from certain asset management products and activities. FSOC must continue to work in an effective manner to meet all of its responsibilities.

Dodd-Frank also established the Council of Inspectors General on Financial Oversight (CIGFO), which I chair as the Treasury Inspector General. The Council facilitates the sharing of information among member Inspectors General with a focus on reporting our concerns that may apply to the broader financial sector and ways to improve financial oversight. As required, CIGFO met quarterly and issued its sixth annual report in July 2016.

As we have stated in the past, the intention of Dodd-Frank is most notably to prevent, or at least minimize, the impact of a future financial sector crisis on the U.S. economy. To accomplish this,

Dodd-Frank placed great responsibility with the Secretary of the Treasury, as Chairman of FSOC. Management's challenge from our perspective is to maintain an effective FSOC process that timely identifies and appropriately responds to emerging risks, particularly in times of economic growth when government action to curtail risky behavior in marketplaces can be unpopular and seen as unnecessary.

### Small Business Jobs Act

A \$30 billion Small Business Lending Fund (SBLF) was established within Treasury to assist financial institutions with increasing the availability of credit to small businesses. It also provided Treasury with \$1.5 billion to allocate to eligible State programs through the State Small Business Credit Initiative (SSBCI). These programs represented key initiatives to support job creation by facilitating increased lending to small businesses.

Under SBLF, Treasury invested approximately \$4 billion in 332 participating banks and Community Development Loan Funds (CDLF), which was intended to stimulate lending to small businesses. As of August 2016, 254 institutions have exited the program redeeming approximately \$3.6 billion of their securities. With dividend and interest rates as high as 13.8 percent, it is expected that remaining bank participants will continue exiting the program, but some of these institutions may have difficulty redeeming their securities. Of the 78 participants remaining in the program, more than half comprise CDLFs, which pay an interest rate of two percent during the first eight years in the program, and nine percent thereafter. While the number of participants has decreased significantly since the SBLF program's inception, Treasury must ensure that dividends and interests owed from remaining participants are paid.

Under SSBCI, Treasury disbursed approximately \$1.4 billion to 57 participating States, territories, and eligible municipalities as of March 2016. These funds may be used for programs that partner with private lenders and investors to extend credit to or invest in small businesses. Treasury must ensure that SSBCI participants are accountable for the proper use of these funds as primary oversight is at the participant level. An additional challenge to Treasury's oversight is that, if the SSBCI program is not reauthorized by Congress, its authority to administer the program ends after fiscal year 2017. As such, Treasury will need to recoup funds our office determines were recklessly or intentionally misused before the program ends.

We recognize that the SBLF and SSBCI programs are reaching maturity. However, Treasury must still exercise sufficient oversight while winding down these programs.

### Housing and Economic Recovery Act

Treasury supports the financial solvency of the Federal National Mortgage Association (Fannie Mae) and the Federal Home Loan Mortgage Corporation (Freddie Mac), which continue to operate under the conservatorship of the Federal Housing Finance Agency. To maintain the positive net worth of these two government sponsored enterprises (GSE), Treasury has invested approximately \$189 billion in senior preferred stock in the two enterprises.<sup>4</sup> While the GSEs have not required additional support since fiscal year 2012, their futures remain uncertain and

---

<sup>4</sup> Treasury's cumulative investment of \$189 billion in the GSEs' senior preferred stock is comprised of approximately \$117 billion in Fannie Mae and approximately \$72 billion in Freddie Mac.



further assistance may be required. If such support is needed, the current funding capacity available to Fannie Mae is \$117.6 billion and available to Freddie Mac is \$140.5 billion.

Treasury must also continue to monitor the underlying assets of its \$7.1 billion investment in the GSEs under the Housing Finance Agency Initiative, which supports State and local housing finance agencies.

Until a solution to address housing finance reform is reached, it is difficult to predict what lies ahead for winding down the GSE investments.

### Recovery Act

Since 2009, Treasury has been responsible for overseeing an estimated \$150 billion of funding and tax relief for programs intended to strengthen the economy through financial stimulus. While funding for non-Internal Revenue Service programs is coming to a close, Treasury continues to oversee awards totaling around \$30 billion under Treasury's payments-in-lieu of tax credit programs – to persons for specified energy properties and to States for low-income housing projects. In this regard, approximately 101,000 recipients remain obligated to comply with the terms of their awards over an extended period of time (5 years for specified energy property payments and 15 years for funded low-income housing projects). The level of risk involved in this program is evidenced by the fact that our Office of Investigations has several open matters involving program participants. Furthermore, Treasury's energy program continues to attract Congressional and media interest.

### RESTORE Act

In response to the 2010 *Deepwater Horizon* oil spill, Congress enacted the RESTORE Act, which among other things, established within Treasury the RESTORE Act Trust Fund. Eighty percent of administrative and civil penalties paid by responsible parties pursuant to the Federal Water Pollution Control Act (Clean Water Act) are to be deposited into the Trust Fund and distributed, as stipulated by the act, for the economic and environmental restoration of the Gulf Coast region.

As of this writing, the Trust Fund received approximately \$936 million as a result of the Federal government's settlements with Transocean and Anadarko defendants as well as interest payments. The Trust Fund is further expected to receive deposits of \$4.4 billion plus interest over a 15-year period from the Federal government's settlement with BP Exploration & Production Inc. Deposits are to begin in April 2017.

Distributions from the Trust Fund are allocated among five components that are managed by three administrators. Treasury is responsible for administering the Direct Component (35 percent) and the Centers of Excellence Research Grants Program Component (2.5 percent). The Gulf Coast Ecosystem Restoration Council (Council)<sup>5</sup> is responsible for managing 60 percent of

---

<sup>5</sup> The Gulf Coast Ecosystem Restoration Council consists of the following members, or designees: (1) at the Federal level, the Secretaries of the Interior, Army, Commerce, Agriculture, the head of the department in which the Coast Guard is operating (currently the Secretary of Homeland Security), and the Administrator of the Environmental Protection Agency; and (2) at the State level, the Governors of Alabama, Florida, Louisiana, Mississippi, and Texas.

the Trust Fund distributions allocated to the Council-Selected Restoration Component (30 percent) and the Spill Impact Component (30 percent). The National Oceanic and Atmospheric Administration (NOAA) administers the Science Program Component (2.5 percent).

Now that funds are beginning to flow from the Trust Fund, potential risks on the horizon include potential irregularities in the awarding of contracts, misallocation of grant proceeds, duplication of funding for projects, and noncompliance with the laws, regulations, or standard operating procedures. Failure to properly monitor funded activities and funding programs that fail to promote the restoration of the Gulf Coast region create additional exposure to the Trust Funds.

In addition to the Trust Fund, there is a multitude of funding sources available for the economic and environmental restoration of the region given the impact of the oil spill to the Gulf Coast region. Managing restoration activities will be difficult as there is no statutory requirement for all affected parties to coordinate restoration activities, and there is no central authority to identify potential overlaps. In its RESTORE Act rule, effective February 12, 2016, Treasury notes that beyond what the RESTORE Act stipulates, it cannot require the Council, NOAA, States, counties, or parishes to coordinate their selection of projects across components in order to achieve particular economic or environmental goals. However, voluntary efforts to coordinate activities are encouraged. Treasury further intends to facilitate these efforts by publishing Direct Component Multiyear Implementation Plans and other information related to the grant programs it administers.

Going forward, it is expected that demands for technical assistance from the Office of Gulf Coast Restoration will increase now that several Direct Component Multiyear Implementation Plans have been accepted by Treasury and a number of Direct Component planning assistance and construction grants have been awarded.

## **Other Matters of Concern**

Although we are not reporting these as management and performance challenges, we are highlighting three areas of concern. Two areas of concern are repeated from last year's letter: (1) currency and coin production and (2) documenting key activities and decisions. In addition, we have added a new area of concern, Enterprise Risk Management.

### Currency and Coin Production

In 2012, we reported on deficiencies with the Bureau of Engraving and Printing's (BEP) production process, which led to 1.4 billion finished NexGen \$100 notes being printed (in 2010) but not accepted by FRB because creasing was detected in some of the finished notes. Although the production problems were identified and sufficiently resolved and FRB began supplying financial institutions with the redesigned NexGen \$100 notes in 2013, BEP and FRB still need to decide on the disposition of the 1.4 billion finished notes that have not been accepted by FRB. Furthermore, BEP plans to redesign the \$20, \$10, and \$5 notes and will need to ensure that the design and production projects are adequately managed to avoid another instance of production deficiencies similar to those identified with the rollout of the \$100 note.

Another matter related to currency redesign that should be kept in mind is meaningful access to U.S. currency for blind and visually impaired individuals. In response to a court ruling on that matter, in 2011 Treasury submitted a three-element approach to provide such access. Two elements of this approach—raised tactile features and large, high-contrast numerals—require changes to the design of currency. The third element is a three-phased program started in 2014 to provide currency readers. The lessons learned from the NexGen \$100 note production process underscore the need for sound and comprehensive project management as BEP undertakes this redesign effort.

Challenges continue to exist with coin production at the U.S. Mint (Mint). For example, the cost of producing penny and nickel coins were double their face value because rising metal prices have resulted in higher production costs. The Mint has undertaken a comprehensive review of U.S. currency to include the production and use of coins, the use of alternative metals, and the suitability of Mint facilities for production.

In addition to concerns over currency and coin production, it is imperative that BEP and the Mint 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 FRB.

#### Documenting Key Activities and Decisions

In prior years, I have cited several audits by my office that highlighted lapses by the Department in maintaining a complete and concurrent record of key activities and decisions. In several audits, we reported ongoing concern over the lack of documentation supporting the selection of financial agents such as those to administer Treasury's investment in Fannie Mae and Freddie Mac and Fiscal Service's Direct Express<sup>®</sup> Debit MasterCard,<sup>®</sup> as well as, Fiscal Service's selection of financial agents to provide banking services to the Federal Bureau of Prisons. Insufficient documentation was also reported with regard to Treasury's consultative role with the Department of Energy's Solyndra loan guarantee and the Office of the Comptroller of the Currency's oversight of foreclosure-related consent orders. 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. Maintaining proper documentation is also in the best long-term interest of Treasury and its component offices and bureaus if actions are later questioned, as they have been. In this regard, appropriate documentation can be as simple as contemporaneous notes providing a record of why decisions were made, the way they were made, and how the Federal Government satisfied itself that the decisions were the best course of action. Also adding to the documentation challenge is the increase in Federal retirements along with the resulting loss of institutional knowledge. We do note that Treasury has issued policy that addresses documentation requirements, such as Treasury Directive 80-05, "Records and Information Management Program." We also believe that policies and procedures are essential to ensure critical functions (1) continue when personnel change and (2) are carried out in a consistent manner in accordance with management's direction. In our view, issues

with maintaining documentation and policies and procedures are a matter of Treasury management and personnel needing to remain aware and vigilant.

Enterprise Risk Management

The Office of Management and Budget's revised Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, requires agencies to develop an ERM capability to integrate strategic planning and review processes and internal control processes. Agencies must begin ERM implementation starting fiscal year 2017 by developing an ERM governance structure and beginning to work on an agency-wide risk profile. This requires close collaboration across all mission and mission-support functions. The challenges highlighted in this letter should be considered as Treasury establishes a comprehensive and effective ERM program.

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