DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

October 30, 2015

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-16-002)

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.

We are reporting five challenges, which are updated from last year.

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

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.

This year, we also combined two Challenges that were reported separately in the previous year's memorandum. Specifically, we incorporated last year's Challenge, "Continued Implementation of Dodd-Frank," into the broader Challenge, "Management of Treasury's Authorities Intended to Support and Improve the Economy." We did this because many requirements directed to Treasury and the Treasury Secretary in the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank) have been addressed, and the offices and functions called for by the Act have now been in place for a number of years.

In assessing the Department's most serious challenges, we remain mindful of external factors that affect Treasury. Congress has not resolved much 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. Other pressures on Federal spending continue, such as the military action against the Islamic State of Iraq and the Levant and continued operations in Afghanistan. The polarized political environment in which the Federal Government has been operating since 2010, with the repeated cycle of budget and debt ceiling stopgaps, has resulted in waste and inefficiency.

In an early draft of this memorandum which was shared with the Department, I included the debt limit impasse as a new challenge for this year because of the immediacy of the need to raise the debt ceiling to avoid potentially catastrophic consequences to the U.S. and world economies from a debt default, and the uncertainty as to the Congressional action in that regard. I removed that challenge in this final memorandum as Congress has passed legislation, as of the date of this writing, for a temporary extension of the debt limit until March 15, 2017. That said, a more long-term solution to the recurring debt ceiling impasse still requires continued Treasury effort. Cyber threats to Treasury operations and the financial sector, which we elevated to a Challenge last year, will continue to be a serious risk for the foreseeable future. Additionally, Treasury administers programs that are inherently high-risk, such as programs to combat terrorist financing. With respect to Dodd-Frank, the mechanisms put in place to promote financial stability have not yet be tested in a time of crisis.

Treasury has, throughout the years, had 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. 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.

2015 Management and Performance Challenges

Challenge 1: Cyber Threats

Cybersecurity represents 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.

In our recent audits of selected Treasury bureaus, we found that security measures were not sufficient at the time to fully prevent and detect vulnerabilities to their networks and 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.

Cyber attacks on financial institutions continue to evolve at an accelerated rate, and include distributed denial of service attacks, phishing attacks, and fraudulent wire payments. 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: 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 (HERA) and the Emergency Economic Stabilization Act (EESA) enacted in 2008, 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 in July 2010. 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 under Dodd-Frank. 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's mission is to identify risks to financial stability that could arise from the activities of large, interconnected financial companies; promote market discipline; and respond to any emerging threats to the financial system.

FSOC accomplished much over the past year. As required, FSOC issued its fifth annual report in May 2015. FSOC also designated one nonbank financial company for supervision by the Board of Governors of the Federal Reserve System (FRB) in December 2014. Additionally, FSOC completed annual reevaluations for the three nonbank financial companies previously designated and did not rescind the designations. In February 2015, FSOC adopted changes related to its process for reviewing nonbank financial companies for potential designation to increase the

transparency of its determinations and to formalize certain practices. Furthermore, FSOC also engaged in work to analyze risks associated with the asset management industry and the potential of such risks to affect U.S. financial stability. 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. Accordingly, CIGFO is an important source of independent analysis to FSOC.

As required, CIGFO met quarterly and issued its fifth annual report in July 2015. CIGFO also established its fourth Working Group in September 2014 to assess FSOC activities related to interest rate risk. The Working Group determined that FSOC monitors interest rate risk on an ongoing basis by facilitating the sharing of financial expertise and information among FSOC members and member agencies and by making annual report recommendations. The Working Group noted that since 2011, FSOC's annual reports to Congress have discussed interest rate risk and recommended actions to address that risk. In that regard, FSOC's 2013 annual report included three interest rate risk recommendations and the 2014 annual report included two interest rate risk recommendations. To that end, the Working Group recommended that FSOC document in its annual reports its rationale for removing previously reported recommendations related to interest rate risk. In the view of the Working Group, the lack of explanation to remove previously reported recommendations created a lack of transparency around the process for removing such recommendations. In response to the Working Group's recommendation, FSOC stated that to the extent that it no longer recommends action related to a risk area identified in the prior annual report, FSOC will consider how to provide additional information regarding the Council's decision and analysis. Going forward, CIGFO will continue to review FSOC operations and efforts to oversee the U.S. financial system.

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 Treasury. This management challenge from our perspective is to maintain an effective FSOC process[1] 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 Lending Fund and State Small Business Credit Initiative

The Small Business Jobs Act created within Treasury a $30 billion Small Business Lending Fund (SBLF) 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

[1] FSOC is supported by the Office of Financial Research and the Federal Insurance Office; both are offices within Treasury.

initiatives of the Administration to support job creation by facilitating increased lending to small businesses.

Under SBLF, Treasury invested approximately $4 billion in 332 participating financial institutions through September 2011, when the investment authority ended. The intent of these investments was to stimulate lending to small businesses. However, participating financial institutions were not required to increase lending activity or report on how Treasury's investment was used. Institutions must pay dividends to Treasury at rates ranging from 1 to 9 percent, which automatically step-up to as high as 13.8 percent in late 2015/early 2016. Eighty-eight (88) institutions have since exited the program redeeming approximately $1.6 billion of their securities as of September 2015. While more institutions are expected to exit the program as dividend rates increase, some institutions may not be able to redeem their securities and exit the program.

Under SSBCI, Treasury disbursed approximately $1.3 billion to 57 participating States, territories, and eligible municipalities as of September 2015. 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.

The challenge to Treasury is to continue exercising sufficient oversight to ensure that (1) funds are used appropriately and intended results are being achieved, (2) SBLF dividends and interest owed are paid, and (3) the SBLF program is wound down as institutions exit. Regarding SSBCI, an additional challenge to Treasury's oversight is that the Department's authority to use SSBCI funds for administrative activities ends in fiscal year 2017, yet States' SSBCI programs will be ongoing.

Bond Guarantee Program

The Small Business Jobs Act provided Treasury with authority to guarantee bonds issued for eligible community and economic development activities. As the program administrator, Treasury's Community Development Financial Institutions (CDFI) Fund experienced challenges in standing up the program, which was eventually established in June 2013. CDFI Fund oversees the issuance of the bonds and the use of the bond proceeds by eligible CDFIs to make financing more accessible in underserved communities. To date, Treasury has issued $852 million in bond guarantees. Given that the program is still in its formative years, our office plans to assess the CDFI Fund's administration of this program.

Housing and Economic Recovery Act and the Emergency Economic Stabilization Act

Through several HERA and EESA programs, Treasury injected capital into financial institutions and businesses.

Under HERA, 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 $187 billion in senior preferred stock in the two enterprises.[2] While the GSEs have not required additional support since fiscal year 2012, their futures remain uncertain and 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 $7.8 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 Fannie Mae and Freddie Mac investments.

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.

Recovery Act Programs

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 should continue 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.

Challenge 3: Efforts to Promote Spending Transparency and to Prevent and Detect Improper Payments

Spending Transparency

The Digital Accountability and Transparency Act of 2014 (DATA Act), signed into law in May 2014, 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;

[2] Treasury's cumulative investment of $187 billion in the GSEs' senior preferred stock is comprised of approximately $116 billion in Fannie Mae and approximately $71 billion in Freddie Mac.

- 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;
- 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.

To fulfill its purpose, the DATA Act imposed certain requirements on the Treasury Secretary, the Director of the Office of Management and Budget (OMB), the Inspectors General of each Federal agency, and the Comptroller General of the United States. In brief, the DATA Act required Treasury and OMB to establish Government-wide financial data standards for reporting spending by Federal agencies and entities receiving Federal funds by May 2015 and further requires 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, including Treasury, are required by the Act to conduct three biennial reviews beginning in 2016 of a statistically valid sample of spending data submitted by the agency and the implementation of data standards by the agency. The Inspector General (IG) community has 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. The IG community is working with the Government Accountability Office and Congress to resolve this issue.

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 (referred to as the data exchange schema) within a short timeframe. As of September 15, 2015, 20 months from the date by which agencies must report Federal spending data in accordance with data standards established under the Act, Treasury and OMB officials have issued the data standards and developed a methodology for agencies to follow when implementing the DATA Act. While an important achievement, much work remains. For example, questions regarding some data standards remain and a final determination regarding the applicability of the DATA Act to certain agencies has not yet been made. In addition, the data exchange schema, processes, and systems needed for agencies to submit data are still being developed. Agencies were recently required to submit DATA Act implementation plans to OMB, which are under review. However, open issues such as those described above may hinder agencies' ability to determine the full scope of the implementation effort required.

Given the broad government-wide implications and critical roles assigned to Treasury by the DATA Act, we consider this a 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.[3]

Detect Improper Payments

In light of the continuing problem with improper payments (estimated at $125 billion, or 4.5 percent of all program outlays, for fiscal year 2014), 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.[4]

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 4: 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

---

[3] Our first audit, completed in May 2015, reported on Treasury's efforts as of October 31, 2014 (Office of Inspector General (OIG), *Treasury Is Making Progress in Implementing the DATA Act But Needs Stronger Project Management* (OIG-15-034; issued May 19, 2015)). As of this writing, we have three audits in progress: (1) a continued review of Treasury's government-wide DATA Act efforts, covering efforts through May 31, 2015; (2) a review of Treasury's establishment of a Data Transparency Office and enhancement of the USASpending.gov website; and (3) a "readiness" review of Treasury as a reporting entity under the DATA Act.

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

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 laws collectively known as the Bank Secrecy Act (BSA). The Financial Crimes Enforcement Network (FinCEN) is the Treasury bureau responsible for administering BSA, while Treasury's Office of Foreign Assets Control (OFAC) administers U.S. foreign sanction programs.

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. To this end, 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. FinCEN issued a notice of proposed rulemaking to that effect in July 2014, "Customer Due Diligence Requirements for Financial Institutions." In August 2015, pursuant to BSA, FinCEN issued a notice of proposed rulemaking to prescribe minimum standards for anti-money laundering programs to be established by certain investment advisers and to require such investment advisers to report suspicious activity.

More recently, 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 October 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.[5] 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

[5] 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 5: Gulf Coast Restoration Trust Fund Administration

In response to the Deepwater Horizon oil spill, Congress enacted the Resources and Ecosystems Sustainability, Tourist Opportunities, and Revived Economies of the Gulf Coast States Act of 2012 (RESTORE Act). This law established within Treasury the Gulf Coast Restoration Trust Fund (Trust Fund) and requires Treasury to deposit into the Trust Fund 80 percent of administrative and civil penalties paid by responsible parties pursuant to the Federal Water Pollution Control Act (Clean Water Act). The funds are to be distributed for environmental and economic restoration activities affecting the Gulf Coast States (Alabama, Florida, Louisiana, Mississippi, and Texas). To date, the Trust Fund received approximately $816 million from the Federal Government's settlement with the Transocean defendants. In July 2015, BP Exploration & Production Inc. (BPXP), agreed to settle with the Federal Government and the Gulf Coast States resulting in approximately $4.4 billion plus interest expected to be deposited into the Trust Fund over a 15-year period.

Under the RESTORE Act, money from the Trust Fund is allocated to five components:

- Direct Component (35 percent) – administered by Treasury for allocation in equal shares to the Gulf Coast States for ecological and economic restoration of the Gulf Coast region;
- Council-Selected Restoration Component (30 percent) – administered by the Gulf Coast Ecosystem Restoration Council (the Council)[6] for allocation to Gulf Coast States and Federal agencies, pursuant to a comprehensive plan approved by the Council, to undertake projects and programs using the best available science that would restore and protect the Gulf Coast region's natural resources, ecosystems, fisheries, marine and wildlife habitats, beaches, and coastal wetlands;
- Spill Impact Component (30 percent) – administered by the Council for allocation to the Gulf Coast States for eligible oil spill restoration activities, pursuant to the Council's approval of the States' plans to improve the ecosystems or economy of the Gulf Coast region, using a regulatory formula;
- Science Program Component (2.5 percent) – administered by the National Oceanic and Atmospheric Administration for its Gulf Coast Ecosystem Restoration Science, Observation, Monitoring, and Technology Program. This program is to carry out research, observation, and monitoring to support the long-term sustainability of the

[6] 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.

ecosystem, fish stocks, fish habitat, and the recreational, commercial, and charter fishing industry in the Gulf of Mexico; and

- Centers of Excellence Research Grants Program Component (2.5 percent) – administered by Treasury for allocation in equal shares to the Gulf Coast States for competitive grant awards to nongovernmental entities and consortia in the Gulf Coast region, including public and private institutions of higher education, to establish centers for excellence to conduct Gulf Coast region research.

The RESTORE Act prescribes how funds will be distributed and gives Treasury the administrative oversight of the Direct Component and Centers of Excellence Research Grants Program Component. Further, the Act provides the Secretary authority to withhold funds to the Council-Selected Restoration and Spill Impact Components if certain conditions in the Act are not met, including compliance with procurement rules and regulations.

Treasury made significant progress in establishing a grants program with the stand-up of the Office of Gulf Coast Restoration. However, challenges remain. The foremost challenge is the demand on Treasury to provide technical assistance to grant applicants as they seek interpretation of regulations and application guidelines and develop multiyear implementation plans. Furthermore, many local governments seeking technical assistance are not experienced as direct recipients of Federal financial assistance.

Going forward, Treasury needs to consider the impact of the proposed settlement with BPXP. Now that a more definitive amount and timing of the money that will flow into the Trust Fund has been determined, Treasury, the Gulf Coast States, and impacted local governments are challenged with ensuring existing plans meet the expected funding levels as well as timing of payments.

We continue to meet with Treasury staff and to provide our perspectives on controls as procedures to administer the Trust Fund are developed. Our audit work to date has focused mainly on Treasury's progress in establishing a grants program to administer the Direct Component and Centers of Excellence Component. Additionally, we reviewed internal controls at Gulf Coast State and local government entities applying for Direct Component planning grants as well as reviewed the selection process by the Gulf Coast States to establish Centers of Excellence. The appropriate disbursement and use of RESTORE Act grants will be a focus of our work going forward.

Other Matters of Concern

Although we are not reporting these as management and performance challenges, we want to highlight two areas of concern: (1) currency and coin production and (2) documenting key activities and decisions.

Currency and Coin Production

In January 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 October 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.

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 United States 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. In addition to rising production costs, 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 customer, 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. These audits reported on the selection of financial agents for Treasury's investment in Fannie Mae and Freddie Mac mortgage-backed securities, 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. In 2014, we reported that Fiscal Service's decisions to establish the Direct Express® Debit MasterCard® program and select the program's financial agent were reasonable. However, its analyses and documentation of those decisions should have been more complete. More recently, we reported a similar situation with two financial agents selected by Fiscal Service to provide banking services to the Federal Bureau of Prisons. In response to this audit, Fiscal Service stated that it was refining and updating its policies and procedures for selection of financial agents, as well as maintaining related documentation. We believe the corrective actions undertaken by Fiscal Service are important to promote transparency and confidence in Treasury's use of financial agents.[7]

In another audit however, when we reported that OFAC lacked policies and procedures for a critical mission function—the implementation of a sanctions program—OFAC's response

[7] OIG, *Former Federal Inmate Debit Card Fees Were Comparable with Other Card Programs, but Documentation Supporting Financial Agent Agreements Was Lacking* (OIG-15-048; Sep. 17, 2015)

was that its current practices were sufficient. We were disappointed with OFAC's response and are presently pursuing this issue through the Department's audit resolution process.[8]

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 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.

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: Brodi Fontenot
Assistant Secretary for Management

[8] OIG, *Libyan Sanctions Case Study* (OIG-16-001; Oct. 26, 2015)