DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

October 15, 2018

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-19-004)

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). In this year's memorandum, my office continues to report the following four challenges, which are repeated and updated from last year.

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

While we continue to report these challenges, we acknowledge the Department's accomplishments and efforts over the past year to address these most critical matters as noted within each challenge discussed. In addition to the above challenges, we are reporting our elevated concerns about two matters: (1) currency and coin production at the United States Mint (Mint) and the Bureau of Engraving and Printing (BEP) and (2) excise tax reform's impact on the Alcohol and Tobacco Tax and Trade Bureau (TTB).

2019 Management and Performance Challenges

Challenge 1: Operating in an Uncertain Environment

As reported in prior year's memorandum, we are mindful of external factors and future uncertainties that affect the Department's programs and operations. Among the most notable were 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 included long-term workforce plans that are in alignment with their strategic plans. [1] These plans were to include proposals in four categories: eliminate activities; restructure or merge; improve organizational efficiency and effectiveness; and workforce management. Treasury submitted its plan to OMB in September 2017, which included cross-agency initiatives and Treasury-specific reforms. In June 2018, after consideration of all

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

Agency Reform Plans, OMB developed its comprehensive "Government–wide Reform Plan and Reorganization Recommendations" (Government–wide Reform Plan) to reorganize the Executive Branch. [2]

After considering Agency Reform Plans, OMB made agency-specific recommendations in its Government–wide Reform Plan that would merge functions with similar missions across agencies. As proposed by Treasury in its Agency Reform Plan, the Government-wide Reform Plan includes a recommendation to transfer alcohol and tobacco responsibilities from the Bureau of Alcohol, Tobacco, Firearms and Explosives within the Department of Justice to TTB in order to leverage the expertise and resources of TTB. The plan also considers Treasury as the agency for carrying out the Office of Personnel Management's responsibilities for retirement processing and servicing. Other potential impacts on Treasury include OMB recommendations to increase coordination and avoid duplication of agency's roles in the areas of small business programs, the housing finance market, and financial literacy and education. Furthermore, the plan also includes a proposal to privatize the United States Postal Service, which is estimated to be insolvent, yet continues to hold a $15 billion unfunded liability to the Treasury's Federal Financing Bank.

Until OMB and agencies begin discussions with Congress to prioritize and refine the proposals in the Government–wide Reform Plan, there is looming uncertainty as to the plan's impact. Nonetheless, the Department must plan for the potential long-term restructuring of certain functions or offices/bureaus and expected budget cuts.

Although not specified in OMB's Government–wide Reform Plan, Treasury proposed to merge specific functions performed by both BEP and the Mint as part of its Agency Reform Plan and fiscal year 2019 Congressional Budget Justification. The merger would simplify particular tasks by migrating BEP's online numismatic sales and marketing presence to the Mint's recently modernized E-commerce infrastructure and services platform, and centrally coordinating non-IT procurements to create economies of scale and reduce expenses. As both bureaus are manufacturing organizations, Treasury expects to gain efficiencies through leveraging acquisition commonalities and procurement expertise, consolidating procurement authority, and generating annual cost savings. Although OMB has approved the merger plan, funding the consolidation is contingent on Congressional approval. In anticipation of this, the Office of Procurement Executive is working with managements of BEP the Mint to develop an implementation plan to complete the consolidation of functions by December 2019. Challenges exist with this consolidation because of known systemic issues with BEP's contract administration practices. In addition, other challenges can be expected when consolidating these functions such as, personnel relocation, facility plans, future information systems operations, combined funding arrangements, acquisition regulation requirements, and continued legal support. Outstanding procurement issues at BEP should be considered in planning for the consolidation.

Tackling these and other critical matters at hand could be more challenging as Presidentially-appointed, Senate-confirmed leadership positions and other key senior level positions within the Department remain vacant. There were noted improvements over the past year in filling certain vacancies within the Office of Terrorism and Financial Intelligence (TFI). Specifically, TFI filled several long standing vacancies including the Assistant Secretary for the Office of Intelligence and

[2] OMB, *Delivering Government Solutions in the 21st Century, Reform Plan and Reorganization Recommendations* (June 2018)

Analysis and the Director of the Financial Crimes Enforcement Network (FinCEN). That said, human capital management overall has become higher-risk as the lengthy security clearance process causes significant delays onboarding highly-skilled individuals to fill critical positions across Treasury.

The backlog of background investigations in the clearance process has been a growing concern government-wide. In its March 2018 testimony, the Government Accountability Office (GAO) reported its January 2018 designation of the security clearance process as a high-risk area because it is the highest management risk in government.[3] This has been contributing to difficulty in recruiting cybersecurity personnel as our previous audits of select Treasury bureaus found 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's and OMB's observations of agencies' impairments. Although progress has been made filling some positions, it is essential that the vacancies Treasury-wide be filled as quickly as possible to avoid potential skill gaps, which could lead to further challenges in meeting key program missions and performing succession planning. The lengthy hiring and backfill timelines are negatively impacting existing personnel's ability to carry out bureau programs.

Along with the uncertainty of OMB's Government–wide Reform Plan, Treasury continues to be challenged with new responsibilities. Most recently, Treasury was tasked to administer a new program authorized by the Social Impact Partnerships to Pay for Results Act[4] (SIPPRA). This program was created to direct Federal funds to State and local government partnership programs that is intended to result in measurable social benefits. Treasury, in consultation with the newly created Federal Interagency Council on Social Impact Partnerships, is responsible for administering the program including, but not limited to, publishing the first requests for SIPPRA proposals by February 2019.

The impact of these challenges and the uncertainties of OMB's Government–wide Reform Plan 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. It is essential that new programs and reforms be managed and communicated effectively such that performance and accountability can be improved and missions can still be met throughout the Department.

Treasury must operate in the repeated cycle of budget and debt ceiling stopgaps. As I have 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 suspend the statutory debt limit through March 1, 2019, no long-term solution has been found.

Challenge 2: Cyber Threats

Over the past year, Treasury has maintained steady progress in addressing the continual and on-going challenges that the Federal Government and private sector face, including the threat of

[3] GAO, *Personnel Security Clearances, Additional Actions Needed to Implement Key Reforms and Improve Timely Processing of Investigations* (GAO-18-431T: March 2018)
[4] Public Law 115-123, Bipartisan Budget Act of 2018, Title VIII (February 9, 2018)

ransomware and difficulty obtaining cybersecurity personnel. While a good patch management program assists with defending against attacks such as ransomware, Treasury must continue to ensure its layered defenses (such as network segmentation) are in place and functioning properly to reduce the spread and potential damage malware can do when there is no patch available, or for when that first line of defense fails. Additionally, in our prior audits of select Treasury bureaus, we found 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's and OMB's observations of agencies' impairments as noted in challenge 1. In response to our prior year challenges memorandum, Treasury reported progress in reducing the cybersecurity vacancy rate from fiscal year 2016 to fiscal year 2017, which is a positive step in addressing the lack of resources although the government-wide challenges for retaining this workforce still remain as reported in 2016 by GAO[5] and by OMB in the Cybersecurity Sprint. [6]

Cybersecurity continues to be a long-standing and serious challenge facing the Nation. 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 ongoing challenges for Treasury to fortify and safeguard its internal systems and operations along with 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 continue to increase in frequency and severity, in addition to continuously evolving. As the tools used to perpetrate these attacks become easier to use and more widespread, the less technological knowledge and fewer resources are needed to launch successful attacks of increasing sophistication. 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 third-party cloud service providers are properly

[5] GAO, *Actions Needed to Address Challenges* (GAO-16-885T; issued September 19, 2016)
[6] OMB, M-16-15, *Federal Cybersecurity Workforce Strategy* (July 12, 2016). The goal of the Cybersecurity Sprint was to rapidly improve cybersecurity across the workforce, and also included a review of cybersecurity polices, plans, and procedures.

protected. Issues related to management of cloud systems have been reported in last three consecutive Federal Information Security Modernization Act of 2014[7] audits (fiscal years 2015, 2016, and 2017). Issues included a cloud system with a system security plan that did not address all required security controls, nor did the contract with the third-party cloud service provider address all Federal Risk and Authorization Management Program (FedRAMP) [8] requirements. For another cloud system, required periodic user access reviews were not performed. In another case, risk acceptance for performing security scans less frequently than the standard required was not documented.

As of this writing, Treasury is in the process of implementing the Federal government-wide Continuous Diagnostics and Mitigation program spearheaded by the Department of Homeland Security (DHS). This program is aimed at providing agencies with the capabilities and tools needed to identify cybersecurity risks on an ongoing basis, prioritize these risks based on potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first. The program is organized into four phases that build upon each other, and has required a great deal of coordination within Treasury and also between Treasury and DHS in order to obtain and install the software and tools necessary to support the program. On the horizon, Treasury will be challenged in supporting OMB's plans to implement the activities set forth in the *IT Modernization Report to the President*,[9] such as consolidation and standardization of email services within and across Federal agencies. In order to address these upcoming requirements, Treasury will need to continue to balance cybersecurity demands, the need to modernize and maintain its information technology (IT) systems, and the need to maintain compliance with existing and additional requirements during a time of uncertain budgetary funding. In the case of the Bureau of the Fiscal Service (Fiscal Service), management noted that the modernization of its IT systems is still a work in progress and Fiscal Service management is working with the Assistant Secretary for Management and the Chief Information Officer to ensure modernization of its IT systems align with Treasury's key initiatives.

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

Over the past year, TFI has remained dedicated to countering the ability of the financial networks that support terrorists, organized transnational crime, weapons of mass destruction proliferators, and other threats to international security through intelligence analysis, sanctions, and international private-sector cooperation. Members of the TFI staff chair the U.S. delegation to the Financial Action Task Force (FATF), which is an international policy-making and standard-setting body dedicated to combating money laundering and terrorist financing. FATF found the U.S. Anti-Money Laundering and Combating the Financing of Terrorism framework, which Treasury is responsible for administering, to be well developed and robust. [10]

In 2017, TFI components, along with U.S. foreign partners also established the Terrorist Financing Targeting Center. This center, co-chaired by the United States and Saudi Arabia, is a new initiative

[7] Public Law 113-283 (December 18, 2014)
[8] FedRamp is a government-wide program that standardizes the approach used for security assessments, authorizations, and continuous monitoring for cloud services.
[9] American Technology Council, *IT Modernization Report to the President*, issued December 13, 2017.
[10] FATF, *Anti-money laundering and counter-terrorist financing measures United States Mutual Evaluation Report*, (December 2016)

that brings together every country under the Gulf Cooperation Council, deepening their existing multilateral cooperation by coordinating disruptive action, enhancing information sharing, and institutionalizing capacity-building to target terrorist financing networks that pose national security threats to the United States and the Gulf nations.

As previously reported, identifying, disrupting, and dismantling the financial networks that support rogue regimes, terrorist organizations, transnational criminal organizations, and other threats to the national security of the United States and our allies continues to be challenging as TFI's role to counter these financial networks and threats has grown because its economic authorities are key tools to carry out U.S. policy. Additionally, criminals and other bad actors evolve and continue to develop more sophisticated money laundering methods. To address this growing demand, TFI requested approximately 100 new positions for fiscal year 2019.

TFI's authorities are key tools in implementing U.S. policy to pressure foreign countries and regimes, such as North Korea, Russia, and Iran, and terrorist groups, such as the Islamic State of Iraq and Syria (ISIS) through the use of designations and economic sanctions. The recent passage of the Countering America's Adversaries Through Sanctions Act[11] provides TFI with another avenue to pursue sanctions against these regimes. TFI has significantly increased sanctions against North Korea for missiles testing and it serves a critical role in the United State's maximum economic pressure campaign. TFI also increased sanctions against Russia given recent allegations of interference with the 2016 U.S. election, malign activities in Ukraine, and support of the Government of Syria. As a result of the U.S. decision to withdraw from the Joint Comprehensive Plan of Action (JCPOA),[12] TFI re-imposed nuclear related primary and secondary sanctions, subject to certain 90 and 180 day wind-down periods for activities involving Iran. TFI continues to designate Iranian individuals and entities related to its ballistic missile program, terrorist activities, human rights violations, and Syria-related targets.

TFI's counter-terrorism designations disrupt the financial networks that support terrorist organizations. Disrupting terrorist financing depends on a whole-of-government approach and requires collaboration and coordination within Treasury and with other Federal agencies. Collaboration and coordination are key to successfully identifying and disrupting all of these financial networks and meeting TFI's mission. This effort requires effective and efficient working relationships among components within TFI and the Intelligence Community. In an effort to effectively implement U.S. policy and disrupt these financial networks, TFI is moving towards a more collaborative approach to achieve its mission. However, we noted in the past that TFI can make improvements in the area of coordination.

Effective coordination and collaboration and TFI's ability to effectively gather and analyze intelligence information requires a stable cadre of experienced staff. In an effort to improve coordination and stabilize its workforce, TFI filled long standing vacancies such as the Assistant Secretary of Intelligence and Analysis, which is a key leadership position that had been vacant for approximately 2 years. As noted above, TFI requested approximately 100 new positions for fiscal

[11] Public Law 115-44 (August 2, 2017)

[12] In July 2015, an international coalition, comprised of China, France, Germany, Russia, the United Kingdom, and the United States and Iran reached the JCPOA to ensure that Iran's nuclear program would be exclusively peaceful. The JCPOA provides a long-term, multiphase commitment that deters Iran's path to build a nuclear weapon and imposes rigorous inspections and transparency measures to verify that Iran cannot pursue a nuclear weapon. In May 2018, it was announced that the United States would cease participation in the JCPOA.

year 2019, which will be difficult to fill if approved because of the expertise essential to these positions and length of time to process required security clearances. The security clearance process has significantly impacted Treasury's human capital management as noted in our first challenge and is a systemic issue government-wide.

Stability, experienced leadership, and coordination within TFI is imperative to enhance information gathering and intelligence analysis and increase efficiency. Given the criticality of Treasury's mission, its role to carry out U.S. policy, and resource constraints, 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

Given the broad implications and critical roles assigned to Treasury by the Digital Accountability and Transparency Act of 2014 (DATA Act), we consider this an ongoing high risk implementation project and management challenge. The DATA Act, in part, 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, [13] and the Comptroller General of the United States, as well as Federal agencies and their respective Inspectors General. Several of these mandates have been successfully met to include, most notably, the standardization of 57 Government-wide financial data elements for Federal funds made available to or expended by Federal agencies and entities receiving Federal funds. While there have been successes to date, there is still much to do.

On April 28, 2017, Treasury's Deputy Chief Financial Officer successfully submitted and certified the Department's fiscal year 2017, second quarter financial and award data in the DATA Act broker (broker) for publication on USAspending.gov. However, in our November 2017 audit report, we identified issues with the submission. Specifically, we identified incorrect reporting of Fiscal Service's Administrative Resource Center's[14] customer agency information.[15] Treasury's DATA Act program management office (PMO) and OMB have been working to address this issue and have proposed a solution to ensure that Federal Shared Service Providers' customer agencies' data submissions are properly categorized in the submission and ultimately on USAspending.gov for the first quarter of fiscal year 2019. Further, we identified inaccuracies in the Department's data submission that were a result of how the broker extracts data from external award reporting systems Government-wide. While these inaccuracies are attributable to root causes beyond the Department's control, removal of these Government-wide issues did not significantly change the

[13] Treasury's Government-wide implementation efforts under the DATA Act are led by its Data Transparency Office at the Bureau of the Fiscal Service, also referred to as the program management office (PMO) and OMB's Office of Federal Financial Management. This Government-wide effort is separate and distinct from the Department's DATA Act reporting requirements.

[14] ARC is a Federal Shared Service Provider operating under agreements with other departments, agencies, and bureaus known as customer agencies to provide information technology, human resources, financial, or other services.

[15] OIG, *Treasury Continues to Make Progress in Meeting DATA Act Reporting Requirements, But Data Quality Concerns Remain* (OIG-18-010R November 8, 2017)

overall accuracy rate for the financial and award data the Department submitted to the broker for publication on USASpending.gov. We note that Treasury's PMO reported that these known Government-wide issues have been resolved. We plan to follow up on these matters in future audit work.

On May 9, 2017, Treasury's PMO, in consultation with OMB, met its second Government-wide 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 within three years after enactment of the DATA Act.

Since last year's memorandum, the Department continued to align its systems and execute a comprehensive governance framework to meet the submission and certification requirements of the DATA Act. Additionally, Treasury's PMO continued to refine its processes to address Government-wide implementation challenges through corrective actions to improve data quality for Federal spending transparency. 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 implementation efforts both Government-wide and Department-wide.

Detect Improper Payments

In light of the continuing government-wide problem with improper payments (estimated at $141 billion, or 4.5 percent of all program outlays, for fiscal year 2017), the Federal Government intensified efforts to reduce improper payments in major Federal programs. The Do Not Pay (DNP) Initiative and the Fiscal Service's DNP Business Center are chief components of efforts designed to prevent and detect improper payments to individuals and entities.

The DNP Business Center provides two services to agencies: the DNP Portal and the DNP Data Analytics Service. The DNP 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 DNP 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.[16] In May 2016, we reported that challenges still existed in obtaining better death information.[17] In October 2016, GAO reported that restrictions on the center's access to SSA's full death data remained in place.[18]

In response to the Federal Improper Payments Coordination Act of 2015,[19] the Fiscal Service entered in to agreements with the Department of Defense and the Department of State to incorporate death data collected by these agencies into the DNP Business Center Working System,

[16] OIG, *Fiscal Service Successfully Established the Do Not Pay Business Center But Challenges Remain* (OIG-15-006; November 6, 2014)
[17] OIG, *Fiscal Service Faces Challenges in Obtaining Better Death Information for the Do Not Pay Business Center, but Alternatives Exist* (OIG-16-042; May 18, 2016)
[18] 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)
[19] Public Law 114-109 (December 18, 2015)

which began receiving this data in September 2017. Additionally, legislative proposals were submitted in January 2017 and February 2017 to obtain authorization to use both the SSA's full death file as well as the National Directory of New Hires. [20] In November 2017, OMB designated six additional databases for inclusion in the to the DNP Business Center Working System to help agencies address a broader range of improper payments beyond what can be detected through DNP Business Center's current data sources.[21]

The DNP 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 an audit in progress to assess the services provided to agencies by the DNP Data Analytics Service.

With its potential to reduce improper payments, the DNP 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 DNP Business Center.

Other Matters of Concern

Although we are not reporting these as management and performance challenges, we are highlighting two areas of concern: (1) currency and coin production and (2) excise tax reform.

Currency and Coin

Challenges continue for BEP with an outdated facility for which it needs legislative authority to purchase land for a new facility in the Washington D.C. area. The current facility has limited capabilities when producing $100 notes and this capacity is necessary to ensure continuity of operations at the bureau. 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's latest biennial report issued in 2016 stated that certain metals are being evaluated to change the composition of the nickel to reduce costs. The Mint continues to study this. The Mint must also ensure strong internal controls are in place to safeguard the integrity and protect U.S. coinage. On January 19, 2018, the Mint recommenced its mutilated coin redemption program, which was suspended in 2016, with procedures to enhance the validation of the sources of these coins and to monitor for proper physical security at all Mint facilities. We are currently performing an audit to determine if these procedures are effective.

[20] The National Directory of New Hires (NDNH) is a national database of wage and employment information operated by the Federal Office of Child Support Enforcement (OCSE). OCSE uses the NDNH primarily to assist states administering programs that improve States' abilities to locate parents, establish paternity, and collect child support. The information in this database is only available to authorized persons or entities for authorized purposes.

[21] The following databases were added: (1) Treasury's Office of Foreign Assets Control's Specially Designated Nationals List (OFAC List), (2) the General Services Administration's System for Award Management (SAM), (3) the Internal Revenue Service's (IRS) Automatic Revocation of Exemption List, (4) the IRS's Exempt Organizations Select Check, (5) the IRS's e-Postcard database, and (6) the commercial database American InfoSource (AIS) Deceased Data.

We found in our recent audit of BEP that it had increased its capabilities in project management which improved governance processes and oversight over note development and note production quality. However, BEP is still challenged with producing the next family of redesigned notes that will incorporate new security and technical features to thwart counterfeiters and identify and implement counterfeit deterrence features in a timely manner to safeguard U.S. currency. According to BEP, this will require expansion of its Western Currency Facility in Fort Worth, Texas. The same is true for BEP's outdated Washington, D.C. facility.

Excise Tax Reform

The Craft Beverage Modernization and Tax Reform of 2017[22] reduced the excise tax rates and increased tax credits on beer, wine, and distilled spirits for a two year period beginning January 1, 2018 through December 31, 2019. Among other things, these changes allow all TTB-regulated breweries, wineries, and distilled spirits plants to benefit from a lower effective tax rate for limited quantities of beer, wine, and distilled spirits produced and removed.[23] Eligibility for the reduced rates and tax credits is capped for controlled groups of entities as well as for entities that are treated as a single taxpayer. TTB has been tasked to develop and implement policies and procedures to enforce the quantity limitations for independent entities, controlled groups, and single taxpayers. TTB needs to ensure that it has implemented internal control with the new policies and procedures to ensure that industry members are appropriately claiming the new tax rates and tax credits offered under the new legislation.

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: David Eisner
Assistant Secretary for Management

[22] Public Law 115-97, Section 13801 (December 22, 2017)

[23] Under prior law, a reduced excise tax rate on beer and tax credits for wine were only available to certain small domestic brewers and small domestic wine producers, and there were no reduced excise tax rates for distilled spirits.